TECHNOLOGIES DE L'INFORMATION
Université de Montréal

Projet 1142

Service de répertoire individuel
et de partage de fichiers

Gestion des accès dans DocUM

Guide préparé par : Joanna Frongillo

Version du 23 novembre 2017

Suivi des modifications

Date	Description
19 juin 2017	• Chapitre 10 S'abonner aux avis d'imprévus des TI
29 août 2017	• Chapitre 6 – Nouvelle version de l'OGLP • Le terme DGTIC a été remplacé par TI (sauf pour les hyperliens)
14 sept.-17	• Chapitre 6.12 - Afficher tous les membres de tous les groupes
8 novembre 2017	Nouveaux chapitres : • Chapitre 6.15 - Afficher le rapport de l'unité (nouveauté) • Chapitre 6.16 – Afficher la liste des comptes invités par statut (nouveauté)
23 novembre 2017	Mise à jour du chapitre 6.15 – Nouveauté dans le rapport de l'unité (limites d'affichage)

Table des matières

1 Introduction et remerciements

Ce guide a été conçu dans le cadre de l'implantation du projet 1142 : *Service de répertoire individuel et de partage de fichiers* qui fait partie de la nouvelle offre de service des technologies de l'information (TI) de l'Université de Montréal.

Il se veut un document de base afin d'aider les unités – où il n'existe aucun responsable des ressources informatiques – à sécuriser l'espace de partage de fichiers.

Il est important de noter que les images qui y sont présentées sont utilisées à titre d'exemple seulement et sont différentes pour chaque unité.

Les pictogrammes suivants peuvent être utilisés afin de faciliter le repérage des :

- Informations importantes
- Trucs et astuces
- Liens URL
- Nouveautés
- Alertes de danger
- Mises en garde quant aux limites
- Note


Nos remerciements

Les membres du projet tiennent à remercier les personnes ci-après nommées pour leur inestimable collaboration dans l'élaboration de ce guide. Votre expérience et vos conseils nous ont permis de mieux connaître la réalité des unités quant à la gestion des espaces DocUM. Grand merci donc à :

- Monsieur Arnaud D'Alayer, Responsable informatique, EBSI
- Monsieur Michel Champagne, Archiviste, DGDA
- Madame Lise Desjardins, Responsable de laboratoires informatiques, MÉDECINE
- Madame Marie-France Lalonde, Responsable de laboratoires informatiques, MÉDECINE
- Les membres du « Soutien aux unités » des TI.

2 Mise en contexte du projet 1142

La prolifération des objets numériques non structurés créés ou modifiés par les employés de l'Université ne peuvent actuellement plus être contenus dans les espaces mis à la disposition du personnel administratif et académique de l'Université. Il est donc essentiel pour l'Université de proposer une nouvelle offre de service qui permettra de répondre à des considérations d'ordre technologique et d'instaurer une meilleure gouvernance et une gestion documentaire commune pour tous. Actuellement, la technologie des serveurs de fichiers est désuète et la capacité de stockage ne peut plus évoluer. Il devient donc urgent de bonifier l'offre de service incluant une solution de stockage robuste, sécuritaire, répondant aux exigences croissantes de stockage et offrant une meilleure gouvernance documentaire.

Le projet 1142 vise à fournir :

- Une nouvelle offre de service de partage de fichiers aux unités incluant :
    - **DocUM** : Un nouveau service de partage de fichiers qui répond mieux aux besoins d'espace des unités et qui repose sur le nouvel environnement de stockage en réseau (NAS) robuste et performant ;
    - **SOC** : Une solution de gestion documentaire basée sur le Système officiel de classification de l'Université de Montréal afin de permettre de simplifier et d'uniformiser l'organisation des documents numériques.
- Un nouveau service aux employés et aux professeurs incluant :
    - **OneDrive Entreprise** : Un répertoire de travail individuel qui repose sur le service infonuagique Office 365 incluant l'outil de synchronisation *OneDrive* ainsi que plusieurs autres fonctionnalités offertes par Microsoft ;

Ce guide traite exclusivement de la sécurisation des espaces de partage de fichiers DocUM.

3 L’organisation des fichiers dans DocUM selon le Système officiel de classification

En 2013 l’Université adoptait la « politique de gestion de l’information ». Cette politique vise à « encadrer la création, l’utilisation, le traitement, la transmission, la valorisation et les conditions d’élimination ou d’archivage de l’ensemble de l’information quel que soit le format sous lequel on la retrouve ou son mode de stockage ou de transmission et en assurer la protection ».

DocUM est un espace de répertoires de partage qui répond mieux aux besoins d’espace des unités et qui repose sur un nouvel environnement de stockage en réseau robuste et performant. Tous les fichiers institutionnels confidentiels, stratégiques et finaux doivent y être déposés. Il remplace les anciens serveurs de fichiers (Ocean, Fama, Prunier, Everest…).

Les TI, en collaboration avec la Division de la gestion de documents et des archives (DGDA), a mis en place un plan de déploiement visant :

1) À structurer les données des unités en respectant les prescriptions légales et réglementaires entourant les règles de gestion des documents selon le Système officiel de classification (SOC) adopté par l’UdeM ;
2) À migrer toutes les données institutionnelles vers DocUM.

La première phase du projet est en cours où les responsables de chaque unité sont rencontrés afin d’évaluer les besoins quant à leur structure de répertoires. Les nouvelles structures (basées sur le SOC) sont créées avec l’aide des membres de la DGDA.

Une formation d’une durée de trois (3) heures et un atelier de travail sont offerts aux membres des unités rencontrées. Toutes les notions vues en formation sont détaillées dans le guide « *Partage de fichiers dans DocUM* ».

4 Responsabilités du coadministrateur de l'unité

La personne responsable des arrivées et départs des employés dans l'unité doit :

- Effectuer la gestion de la structure DocUM ;
- Effectuer la gestion des groupes par l'OGLP.

4.1 Effectuer la gestion de la structure DocUM **(avec son compte ca-unité) -** Chapitre 5

Par l'explorateur Windows,

1. Maintenir à jour la structure personnalisée DocUM ;
2. Appliquer les droits d'accès sur les dossiers de la structure DocUM selon les besoins de l'unité.

4.2 Effectuer la gestion des groupes par l'OGLP **(avec son code d'accès personnel) -** Chapitre 6

Par l'outil de gestion locale des permissions (OGLP),

3. Maintenir à jour le **groupe principal** de l'unité (Accueillir et retirer des personnes dans l'unité) pour donner des accès aux ressources communes de l'unité. Il peut s'agir des ressources suivantes, selon les configurations de chaque unité :
    - L'accès aux imprimantes (à moins qu'il n'y ait des groupes précis d'appliqués sur les imprimantes) ;
    - L'accès au partage de fichiers Everest de façon automatique par le VPN ;
    - L'accès au serveur Exchange pour les dossiers publics de l'unité ;
    - Toutes autres ressources communes de l'unité (exemple l'accès à l'espace wiki de l'unité, si la porte d'entrée est le groupe principal de l'unité)

    Le **groupe principal** ne donne pas accès au partage de fichiers dans DocUM.

4. Créer et maintenir à jour les groupes secondaires.

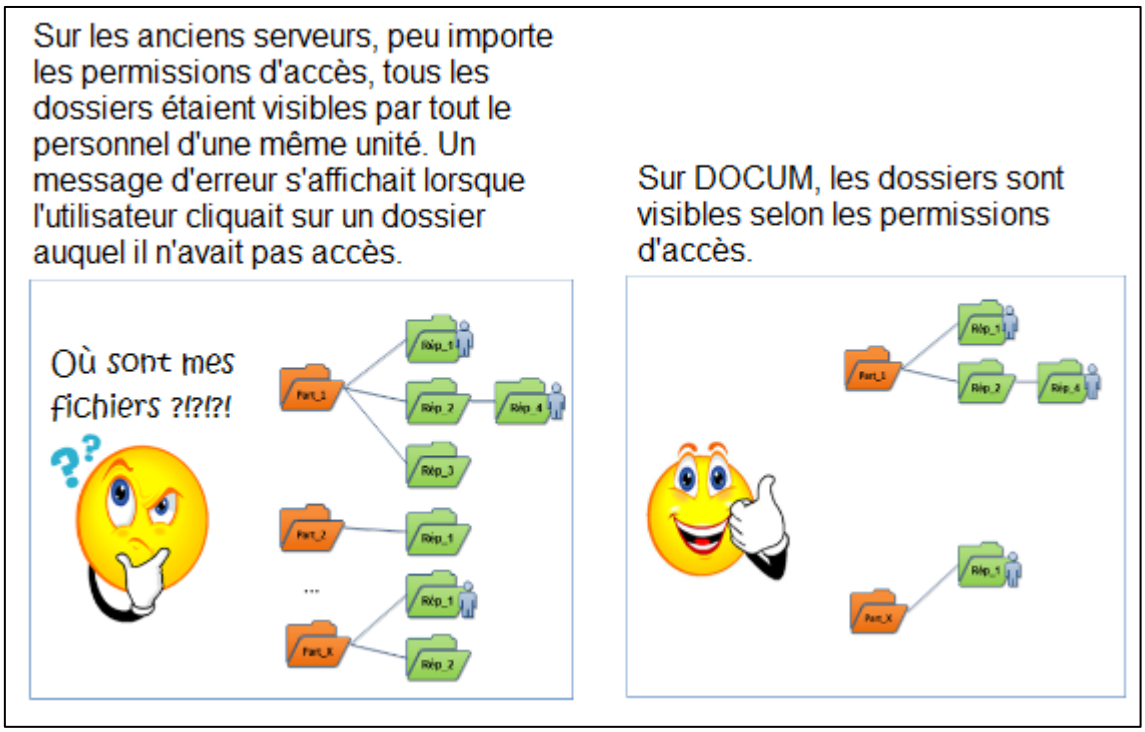
    Il lui faudra imbriquer (ajouter) le ou les groupes secondaires devant avoir accès à la structure DocUM au groupe ***unite-docum*** (porte d'entrée de DocUM).

5 Gestion de la structure DocUM

5.1 Sécurité sur la base des accès (*Access-based Enumeration - ABE*)

La fonctionnalité ABE est désormais active pour DocUM. Elle permet que les utilisateurs ne voient que les dossiers auxquels ils ont des accès ; les autres dossiers ne seront pas affichés.

Lorsque le droit d'accès *« Affichage sur ce dossier seulement »* est appliqué sur un dossier, celui-ci n'est pas propagé par héritage. Il n'est donc pas nécessaire de couper l'héritage pour restreindre les accès.



5.2 Structure personnalisée de dossiers sécurisés

5.2.1 Définition

Définition : ce que nous appelons « secteur », « sous-secteur » ou « activités » se traduit en un « dossier » ou « sous-dossier » dans DocUM.

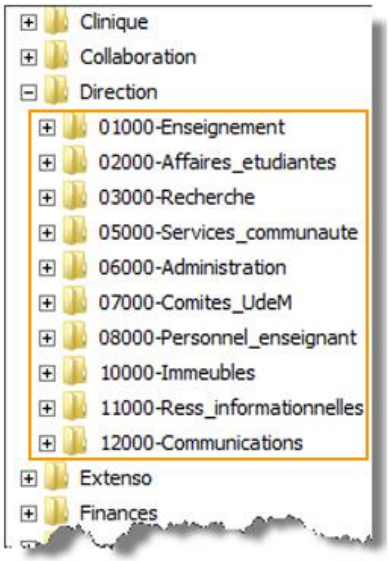
Exemple de secteur :	Academique
Exemple de sous-secteur :	1erCycle
Exemple d'activité :	CollationGrades
Exemple de sous-dossier d'activité :	2016

Ces éléments sont déterminés lors de l'analyse faite avec l'équipe de la DGDA.

5.2.2 Structure à un ou deux niveaux de secteurs

Chaque unité possède sa structure personnalisée. Elle est divisée en secteurs et, dans certains cas, en sous-secteurs. À l'intérieur de ces divisions sont créés les dossiers conformément au Système officiel de classification (SOC) nécessaires à la gestion du secteur, sous-secteur ou activité. Voici des exemples de structure à un (1) niveau et à deux (2) niveaux de secteurs.

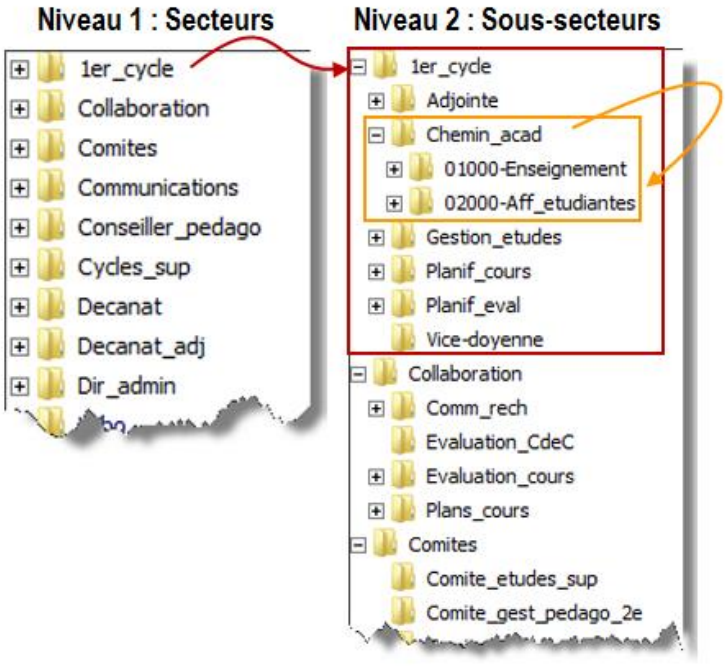
Structure à 1 niveau



Dans l'exemple à droite, nous constatons que l'unité utilise une structure à un seul niveau de secteurs.

Les dossiers « Clinique », « Collaboration », « Direction »…, apparaissent directement en accédant à DocUM. Ces dossiers se trouvent donc au 1er niveau de DocUM.

Les dossiers nommés selon le SOC apparaissent directement sous le 1er niveau de secteur (total des niveaux réels : 2)



Dans l'exemple à gauche, nous constatons que l'unité utilise une structure à deux (2) niveaux de secteurs.

Les dossiers « 1er_cycle », « Collaboration », « Comites »…, apparaissent directement en accédant à DocUM. Ces dossiers se trouvent donc au 1er niveau de DocUM.

Les sous-dossiers « Adjointe », « Chemin_acad » … apparaissent au 2ième niveau.

Les dossiers du SOC du secteur sont placés sous le 2ième niveau (total des niveaux réels : 3).

Il est fortement suggéré de concevoir une structure avec le moins de niveaux possibles. Ceci simplifiera la tâche de la personne responsable de la gestion des droits d'accès.

Étant donné la grandeur de certaines facultés, il pourrait y avoir jusqu'à 3 niveaux de secteurs ; ainsi les dossiers du SOC seraient placés sous le 3ième niveau pour un total de niveaux réels de 4).

Les dossiers associés aux « secteurs » ont été planifiés afin de permettre le partage de fichiers entre les membres d'un même secteur mais aussi pour simplifier la gestion des droits d'accès. Le responsable des accès devra appliquer les droits d'accès directement sur les secteurs (dossiers) et sous-secteurs (sous-dossiers). **Il doit ABSOLUMENT éviter de les appliquer à plus bas niveau.**

5.2.3 Secteur « Collaboration »

Un dossier « **Collaboration** » est souvent créé pour permettre une collaboration entre les membres de secteurs différents. Ainsi, les droits d'accès par secteur ne s'en trouvent pas modifiés. Il est fortement recommandé de ne créer que deux (2) niveaux de sous-dossiers dans celui-ci. L'unité peut en faire un usage temporaire ou permanent.

Utilisation temporaire

Fichiers qui doivent être partagés entre plusieurs secteurs pour une durée limitée. Une fois la collaboration terminée le ou les documents finaux devront être classés dans la structure d'un des secteurs de l'unité et le responsable devra supprimer le dossier de collaboration.

Utilisation permanente

Fichiers qui doivent être partagés de façon permanente (Guides, dépliants…) :

- Par l'ensemble du personnel de tous les secteurs ;
- Par quelques membres de secteurs différents.

Le dossier « Collaboration » ne doit jamais devenir un endroit où l'on peut déposer n'importe quel fichier sous prétexte qu'on ne sait pas trop où ils doivent être classés !

5.3 Recommandations

5.3.1 Gérer les droits d'accès des secteurs en utilisant un ou des groupes

L'utilisation de groupes est essentielle pour maintenir une gestion simple et efficace.

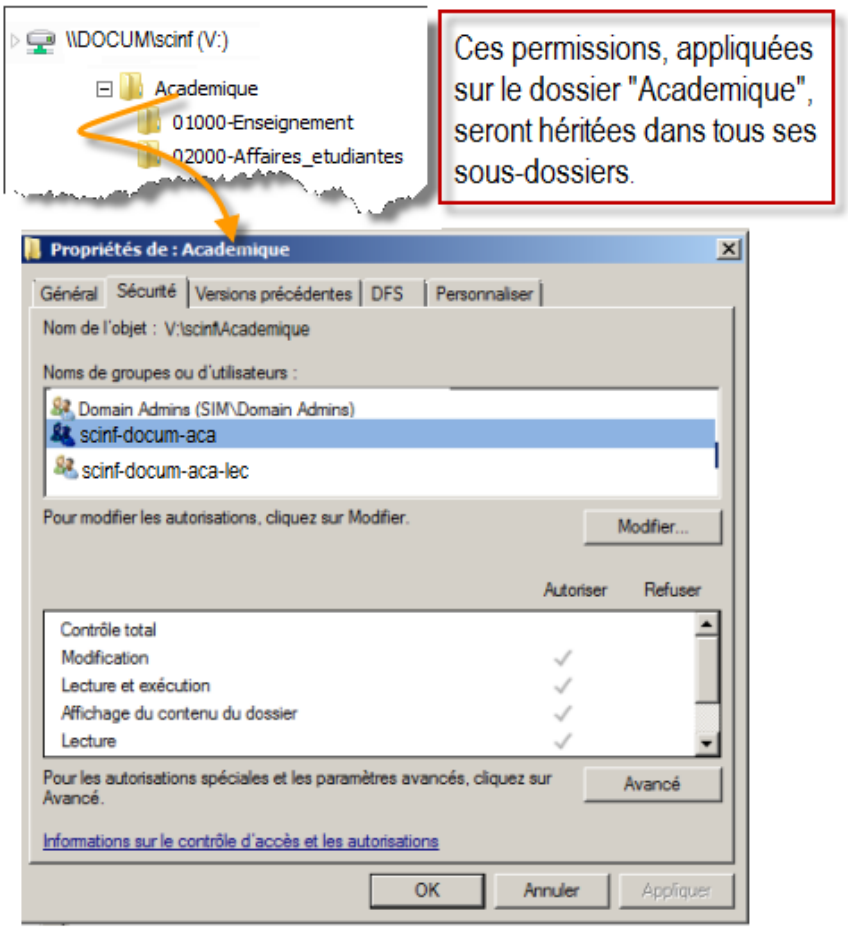
NE JAMAIS OCTROYER DE DROITS À UNE PERSONNE (par son code d'accès) MAIS À UN GROUPE DE PERSONNES. Un groupe peut très bien ne contenir qu'une seule personne.

5.3.2 Créer un groupe par secteur et sous-secteur

Bien que la gestion des accès puisse se faire de plusieurs manières, pour faciliter la tâche de la personne responsable de ces accès, il est recommandé de créer un groupe par secteur et sous-secteur et, au besoin, par droits spécifiques. Les groupes pourront ensuite être appliqués sur les-dits secteurs et sous-secteurs.

Par exemple : le secteur « Academique » est créé à la racine de DocUM pour la Faculté des sciences infirmières. Tous les TGDE doivent y avoir accès en modification et quelques autres employés doivent y avoir accès en lecture seulement. Les groupes suivants seront créés et les accès seront accordés (appliqués) à ces groupes à partir du dossier « Academique » :

Groupe 1 : scinf-docum-aca
Groupe 2 : scinf-docum-aca-lec



En appliquant des permissions pour ces deux (2) groupes dans les propriétés (accessibles par un « clic droit » de la souris sur le dossier) du dossier « Academique » tous les sous-dossiers hériteront des mêmes droits.

Pour raccourcir le nom des groupes, il peut être sous-entendu que les membres d'un groupe ne portant pas la mention « mod » ont des droits de modification.

Il est recommandé également de nommer les groupes en utilisant l'acronyme ***docum*** pour identifier qu'il s'agit d'un groupe donnant des accès à DocUM. Ainsi nous distinguons rapidement l'utilité du groupe.

Le cas de figure au chapitre 5.4 (page 15) vous permettra de bien comprendre l'application des droits d'accès sur une structure à 2 et à 3 niveaux.

5.3.3 Créer des groupes pour donner les accès aux ressources communes

Nous savons que, par défaut, le groupe principal détient les droits d'accès aux ressources communes de l'unité (imprimantes, dossiers publics d'Exchange…). Il arrive parfois que nous voulions restreindre ces accès.

Par exemple, pour restreindre l'accès aux imprimantes le responsable doit :

1. Créer un groupe secondaire nommé *unite-**imprimantes*** (par l'OGLP) et y inclure des membres qui doivent y avoir accès ;
2. Faire appliquer les droits d'accès aux imprimantes à ce groupe par le soutien aux unités des TI (voir coordonnées au chapitre 9 de ce guide).

Si l'accès à chaque ressource de l'unité est géré par des groupes secondaires portant des noms significatifs (unite-**imp**-e624, unite-**imp**-e640, unite-**wiki**, unite-**docum**…), il sera beaucoup plus facile au successeur d'un poste de reconnaître la gestion des permissions établie par son prédécesseur.

5.3.4 Autres options pour la gestion des groupes d'accès

Il est possible d'utiliser des groupes par fonction ou la création de groupes par titre de fonction (par personne). Voici des exemples qui expliquent les deux possibilités.

5.3.4.1 Créer un groupe par fonction

Supposons que l'unité compte six (6) techniciens en coordination du travail de bureau (TCTB) et que ces personnes doivent avoir accès aux mêmes dossiers. Le responsable pourra créer un groupe « unité-fct-tctb » ou « unité-fct-tctb-gr » qui inclura les six codes d'accès des TCTB.

Ce groupe pourra ensuite :

- Être imbriqué dans les groupes donnant accès aux secteurs et sous-secteurs ;
- Être directement appliqué sur les dossiers de DocUM sur un secteur nommé *tctb* par exemple.

5.3.4.2 Créer un groupe par titre de fonction (par personne)

Supposons que l'unité compte six (6) techniciens en coordination du travail de bureau (TCTB), voici comment les groupes seraient créés :

- Six (6) groupes contenant une seule personne chacun sont créés et nommés comme suit :
    - unité-fct-tctb1, unité-fct-tctb2 … unité-fct-tctb6.
- Un groupe général peut être créé et nommé *unité-fct-tctb-gr* où sont imbriqués les groupes *unité-fct-tctb1* à *6*. Ce groupe pourra également être imbriqué dans les groupes donnant accès aux secteurs et sous-secteurs de DocUM.
- Cette méthode permet de gérer les droits d'accès par titre de fonction. Ainsi, lors du départ du TCTB # 3, l'utilisateur sera retiré du groupe *unité-fct-tctb3* et le nouveau TCTB y sera ajouté. De cette façon, il n'est plus nécessaire de savoir quels sont les groupes dans lesquels le nouveau TCTB doit être ajouté.

Attention : Afin d'éviter les problèmes de connexion au VPN et au portail (Site Sharepoint), ne pas dépasser 6 niveaux d'imbrication.

L'une ou l'autre de ces deux méthodes est valable. Il s'agit de bien évaluer ses besoins et de choisir la solution la plus simple tout en respectant le type de gestion qui convient.

1. Les groupes par fonction pourront très bien être appliqués sur d'autres ressources informatiques que DocUM.

2. Les groupes par titre de fonction (par personne) pourraient vous éviter d'avoir à connaître le nom de chaque groupe où un nouvel employé doit être ajouté lors de son arrivée.

Dans le cas où on désire gérer les accès par groupe de fonctions, il est possible d'utiliser les titres de fonction dans le nom des groupes. Consulter la liste des abréviations.

5.4 Exemple d'application de droits d'accès sur une structure DocUM

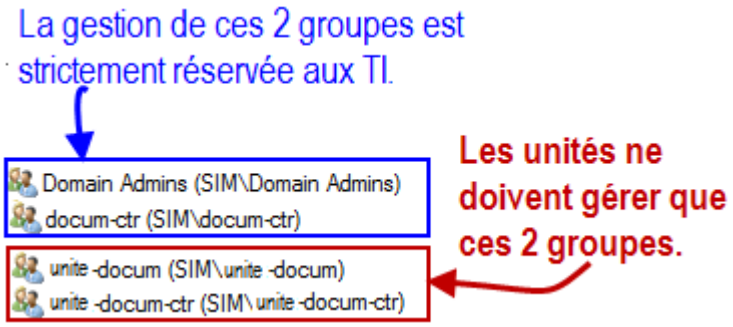
5.4.1 Groupes d'accès par défaut

Par défaut, pour chaque unité, les quatre (4) groupes de sécurité sont appliqués à la racine (dossier du tout premier niveau) de DocUM comme suit :

	Nom du groupe	Sécurité	Qui sont-ils ?
1	Domain admins	Contrôle total	Administrateurs de domaine (TI)
2	docum-ctr	Contrôle total	Membres du soutien aux unités (TI)
3	unite-docum-ctr	Contrôle total	CA de l'unité
4	unite-docum	Affichage sur ce dossier seulement *	Tous les groupes devant avoir accès à un ou plusieurs dossiers de la structure.

L'héritage : Les permissions des trois (3) premiers groupes sont propagées sur tous les dossiers de la structure par héritage. Le dossier « racine » étant le *parent* des sous-dossiers (*ses enfants)*.

* La permission « **Affichage sur ce dossier seulement** » permet d'afficher le dossier ciblé seulement. Aucun fichier ni sous-dossier n'est donc visible pour les membres du groupe. C'est elle qui permet d'effectuer la Sécurité sur la base des accès (voir chapitre 5.1). **Cette permission n'est pas propagée en-dessous même si l'héritage n'est pas coupé**.



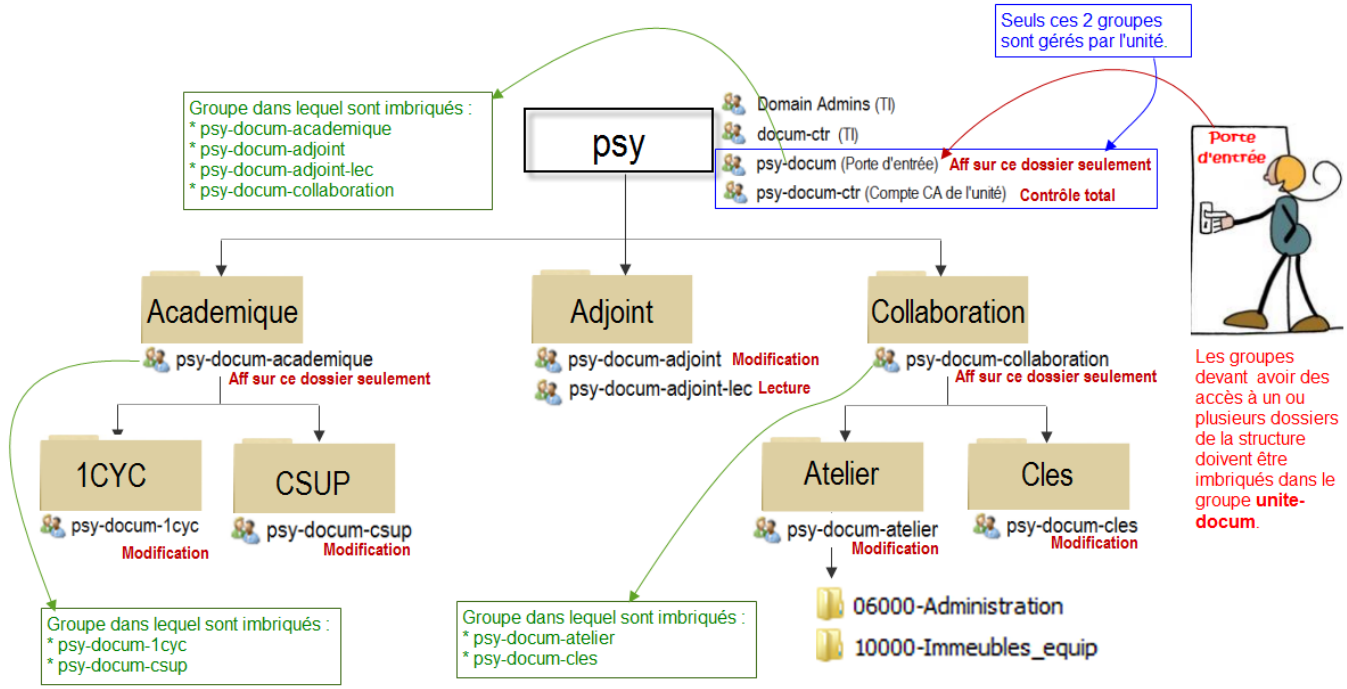
Ces quatre (4) groupes **NE DOIVENT JAMAIS ÊTRE RETIRÉS** de la racine de DocUM.

Un groupe nommé « *unite-docum-avis-quota* » est également créé pour chaque unité. Il ne s'agit pas d'un groupe de sécurité mais d'une simple liste de distribution. Chaque membre de ce groupe (*pas le compte CA mais les comptes d'utilisateurs*) recevra une notification lorsque le quota de l'unité aura atteint 90 et 100 %.

Les informations concernant les quotas (espace utilisé et espace maximum) seront accessibles par le portail employé et ce, pour tous les employés.

Le ou les comptes CA sont membres du groupe nommé « *unite-docum-ctr* ». Il est possible d'y intégrer un code d'accès de façon temporaire en l'absence de la personne responsable de la gestion des accès.

5.4.2 Application des droits pour un cas de figure à 2 niveaux de secteurs



Afin de bien comprendre le modèle suggéré quant à la façon d'appliquer les droits d'accès, nous avons imagé le cas de figure suivant :

- Le département de psychologie compte 3 secteurs – **Academique / Adjoint / Collaboration**.
- Le secteur **Academique** compte 2 sous-secteurs – **1CYC / CSUP**.
- Le secteur **Collaboration** compte 2 sous-secteurs – **Atelier / Cles**.
- Le secteur **Adjoint** ne compte aucun sous-secteur par contre certaines personnes ne doivent avoir que des permissions de lecteur.

Afin de simplifier la lecture de l'image ci-dessus, nous n'avons affiché que les groupes devant être gérés par le coadministrateur (CA) de l'unité. Il est donc sous-entendu que les deux (2) groupes gérés par les TI ont un accès en contrôle total sur la totalité des dossiers de la structure.

Voir explication complète du schéma sur la page suivante.

psy : Dossier racine. Seul l'ajout ou le retrait des membres du groupe *psy-docum* doit être effectué (par l'OGLP) pour donner ou retirer les accès à DocUM. Il s'agit ici de la **porte d'entrée** pour tous les groupes devant avoir accès à un ou plusieurs dossiers de la structure.

Académique : Ce secteur compte 2 sous-secteurs où les droits ne sont pas les mêmes d'un sous-secteur à l'autre. Nous appliquerons donc les droits d'affichage (sur le dossier seulement) sur le dossier **Academique** pour ensuite donner des droits en modification à chacun des sous-secteurs. Les 2 groupes *psy-docum-1cyc et psy-docum-csup* seront imbriqués dans le groupe *psy-docum-academique,* qui lui, sera imbriqué à *psy-docum* (porte d'entrée).

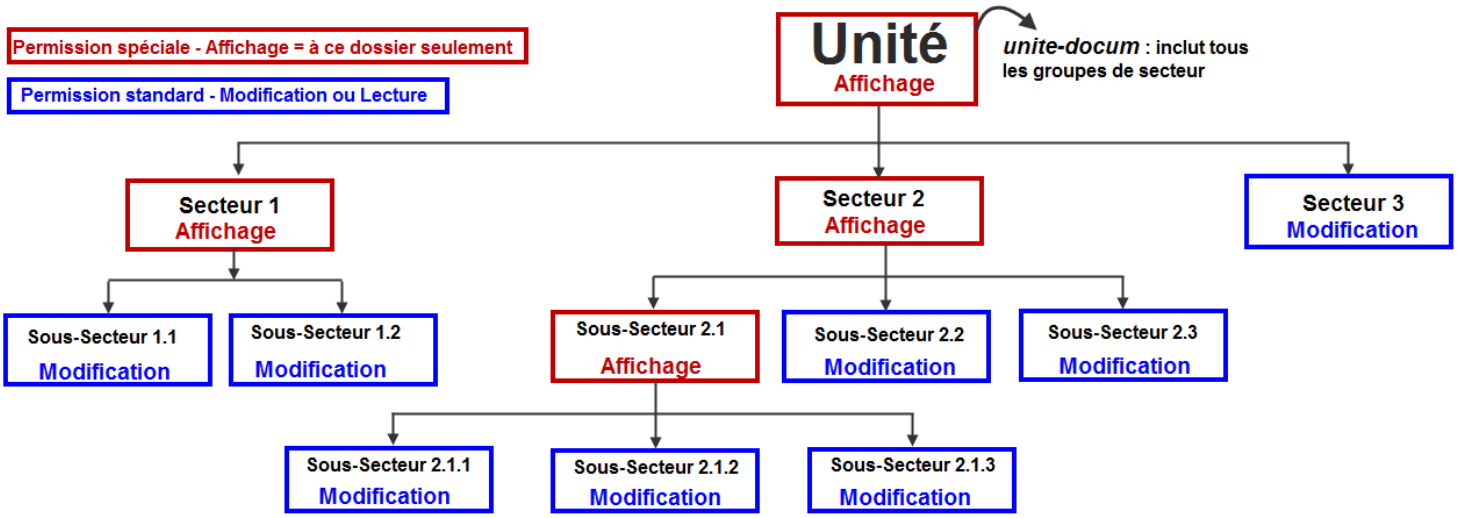
Adjoint : Ce secteur ne compte aucun sous-secteur, par contre une restriction de lecture est requise pour certaines personnes.

Deux groupes sont alors créés, *psy-docum-adjoint* (ses membres auront des droits de modification) et *psy-docum-adjoint-lec* (ses membres auront des droits de lecture seulement). Ces deux groupes seront imbriqués au groupe *psy-docum* (porte d'entrée).

Collaboration : Ce secteur compte 2 sous-secteurs où les droits ne sont pas les mêmes d'un sous-secteur à l'autre. Nous appliquerons donc les droits d'affichage (sur le dossier seulement) sur le dossier **Collaboration** pour ensuite donner des droits en modification à chacun des sous-secteurs. Les 2 groupes *psy-docum-atelier et psy-docum-cles* seront imbriqués dans le groupe *psy-docum-collaboration,* qui lui, sera imbriqué à *psy-docum* (porte d'entrée).

5.4.3 Application des droits pour un cas de figure à 3 niveaux de secteurs

Une faculté pourrait vouloir utiliser 3 niveaux de secteurs plutôt que 2.



Les groupes ayant des droits de modification doivent être appliqués au dernier niveau comme dans l'exemple ci-dessus.

Le groupe ***unite-docum*** contient les groupes suivants :

- **Unite-docum-1**
  Qui lui contient les groupes :
  - unite-docum-1.1
  - unite-docum-1.2
- **Unite-docum-2**
  Qui lui contient les groupes :
  - unite-docum-2.1
    Qui lui contient :
    - unite-docum-2.1.1
    - unite-docum-2.1.2
    - unite-docum-2.1.3
  - unite-docum-2.2
  - unite-docum-2.3
- **Unite-docum-3**

Dans cet exemple, à l'image d'une pyramide, les sous-groupes sont tous imbriqués au groupe du niveau supérieur. Ceci permet aux membres de naviguer dans la structure et cela évite d'avoir à imbriquer tous les sous-groupes de façon individuelle au groupe ***unite-docum à la racine***.

5.5 Procédure pour appliquer des droits d'accès

5.5.1 Ouvrir une session avec le compte ca-unité

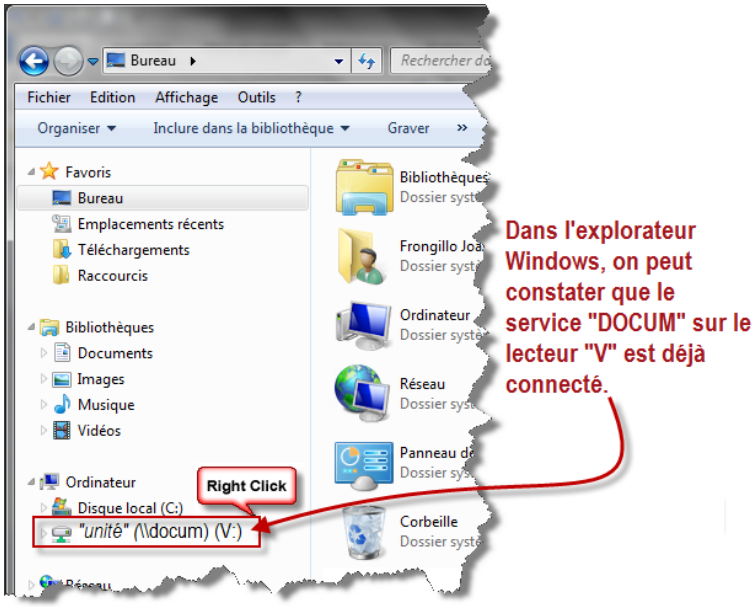
Pour gérer les droits d'accès, il est essentiel que le responsable ouvre une session de travail en s'authentifiant avec son compte **ca-unité**.

5.5.2 Connaître la signification des droits Windows standards

Droits	Description
Affichage du contenu du dossier	Permet de consulter les listes des dossiers/fichiers. Impossibilité d'ouvrir les fichiers.
Lecture	Permet de lire les fichiers/dossiers. Possibilité d'ouvrir les fichiers/dossiers mais pas de les modifier ni d'en créer d'autres.
Lecture et exécution	Permet de lire et d'exécuter des fichiers d'action (fichier dont l'extension est « exe » par exemple). Possibilité d'ouvrir les fichiers/dossiers et d'exécuter les fichiers d'action, mais pas de les modifier ni d'en créer d'autres.
Écriture	Permet d'écrire mais doit être jumelé avec « Lecture ». **NE PEUT PAS ÊTRE DONNÉ SEUL**. Possibilité de créer des nouveaux fichiers/dossiers mais impossibilité de les supprimer.
Modification	Permet d'avoir tous les droits précédents (Affichage du contenu du dossier, Lecture, Lecture et exécution, Écriture) et permet également de supprimer.
Contrôle total	Permet d'avoir tous les droits précédents et permet également de modifier les droits.  **Cette permission ne doit pas être déléguée à des codes d'accès personnels ou des groupes d'utilisateurs, elle est réservée au groupe *unite-docum-ctr* (comptes CA).**

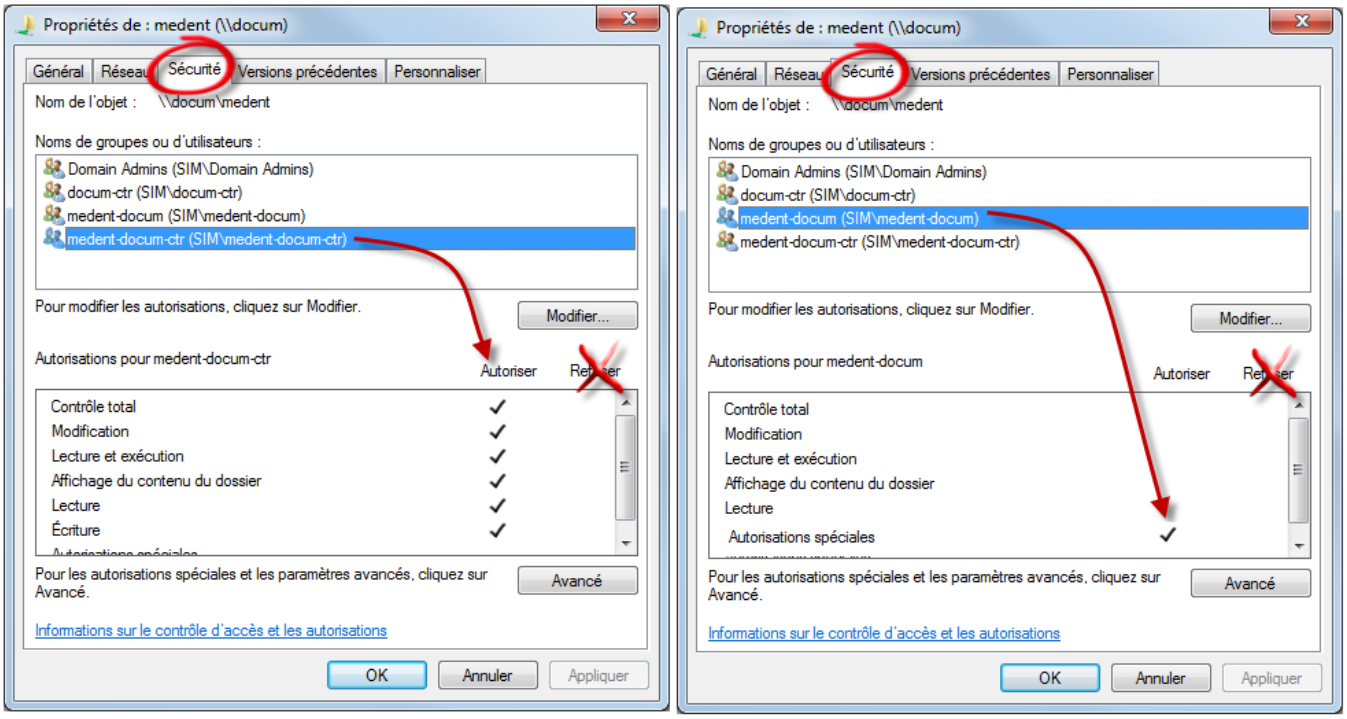
5.5.3 Consulter les droits d'accès de DocUM

Pour consulter les droits de l'espace de l'unité, accéder aux propriétés du lecteur *«Unité» (\\docum) (V:)* par le bouton droit de la souris.



L'onglet « Sécurité » affiche tous les groupes ayant des droits d'accès.

En sélectionnant un groupe dans la partie supérieure de la fenêtre, les droits du groupe s'affichent dans la partie inférieure.



On constate dans l'exemple de gauche que le groupe *unite-docum-ctr* (le compte CA de l'unité) détient le contrôle total alors que dans l'exemple de droite le groupe *unite-docum* détient des *Autorisations spéciales.*

5.5.4 Ajouter/modifier des droits – Autorisations spéciales « Sur ce dossier seulement »

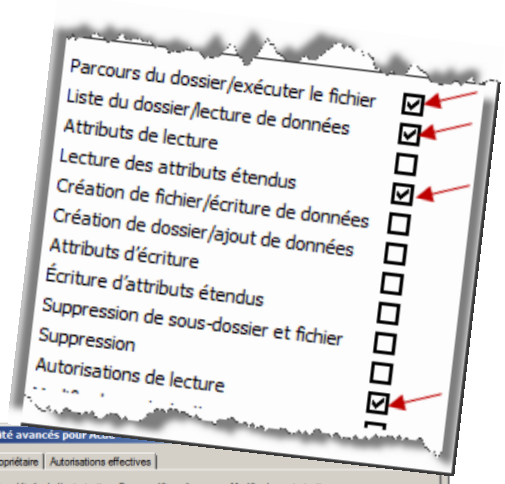
Dans le modèle de structure proposé, plusieurs groupes doivent détenir des permissions que nous avons nommées « ***Affichage sur ce dossier seulement*** ». Il s'agit d'autorisations spéciales qui ne font pas partie des permissions standards. Le droit « *Affichage sur ce dossier seulement* » permet d'ouvrir une porte aux membres du ou des groupes bénéficiant de ce droit particulier. Sans couper l'héritage, seul le dossier ciblé sera visible et non tous les éléments qui se trouvent en-dessous.

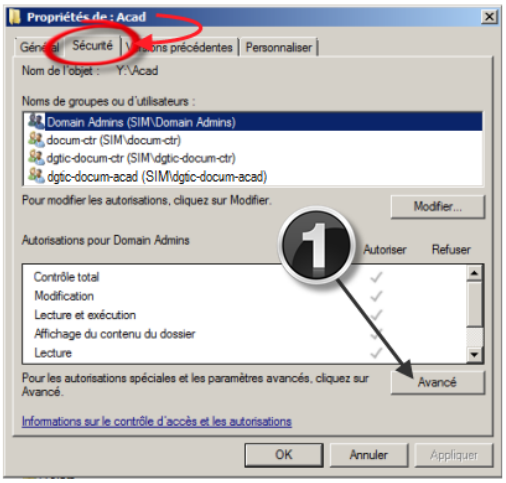
Une fois dans l'onglet *Sécurité* du dossier désiré :

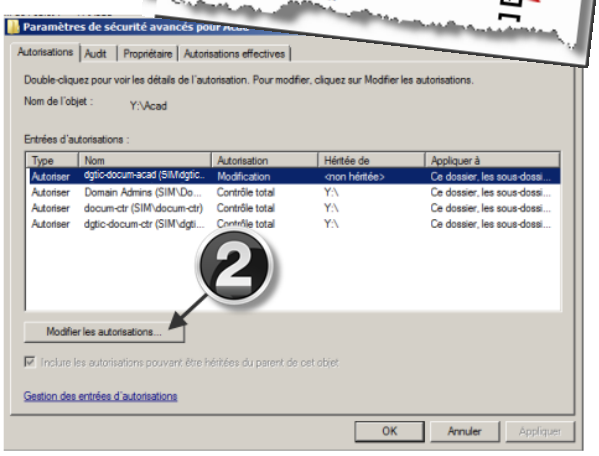
1) Cliquer sur *Avancé*.
2) Cliquer sur *Modifier les autorisations*.
3) Cliquer sur *Ajouter* si le groupe n'existe pas encore ou *Modifier* si le groupe est déjà existant et cliquer sur *OK*.
4) Dans la zone *Appliquer à :* sélectionner ***Ce dossier seulement***

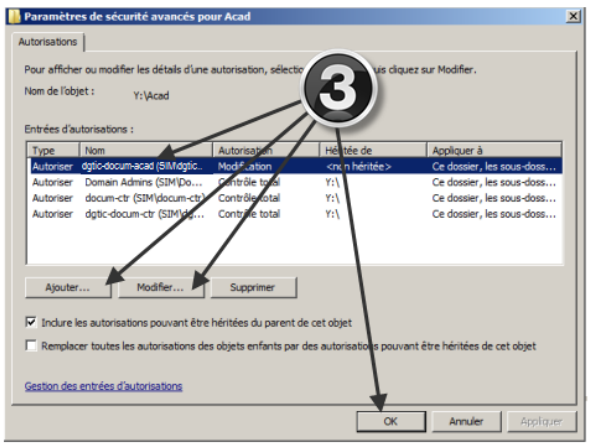
Si cette option n'est pas sélectionnée, il est possible de corriger sans tout reprendre la procédure.

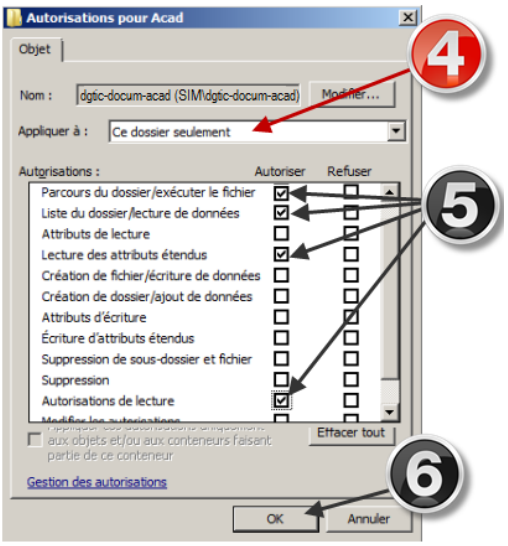
5) Cocher les quatre (4) cases suivantes :
   a. *Parcours du dossier/exécuter le fichier*
   b. *Liste du dossier/lecture de données*
   c. *Lecture des attributs étendus*
   d. *Autorisation de lecture*
6) *Confirmer*.





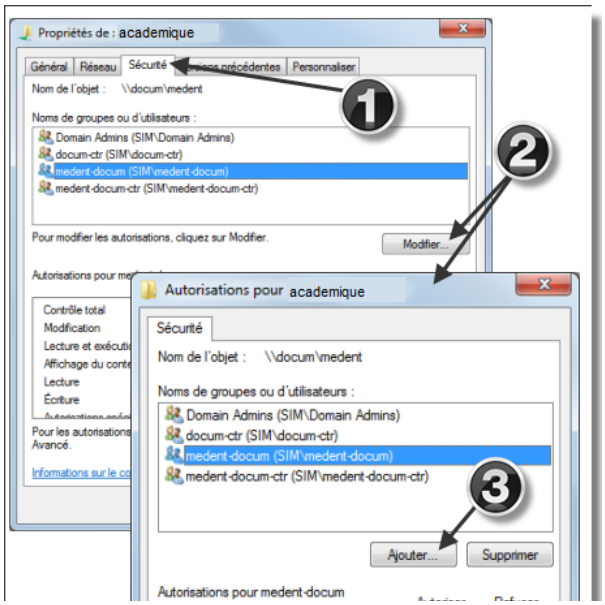




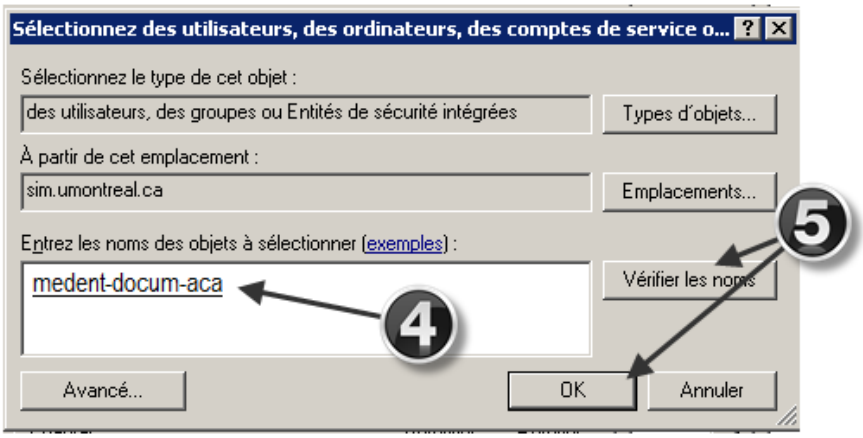


5.5.5 Ajouter des droits de lecture ou de modification sur un dossier

1) Accéder à l'onglet *Sécurité* des propriétés d'un secteur ou sous-secteur (menu contextuel du dossier).
2) Cliquer sur *Modifier*. La fenêtre *Autorisations pour…* s'affiche.
3) Cliquer sur *Ajouter*. La fenêtre *Sélectionnez des utilisateurs, des ordinateurs…* s'affiche.



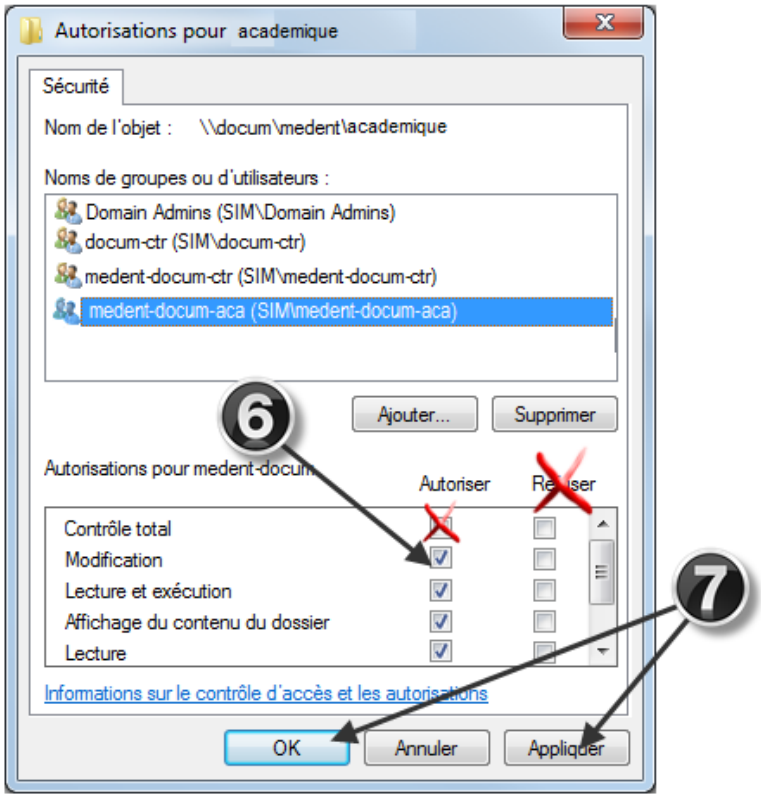
4) Saisir le nom du groupe (en partie ou au complet) dans la zone de texte.
5) Cliquer sur *Vérifier les noms*. S'il existe plus d'une possibilité, choisir le bon groupe et cliquer sur *OK*.
6) Autoriser les droits en cochant les cases appropriées. Les droits sont cumulatifs.



Il est conseillé de ne jamais « Refuser » des droits.

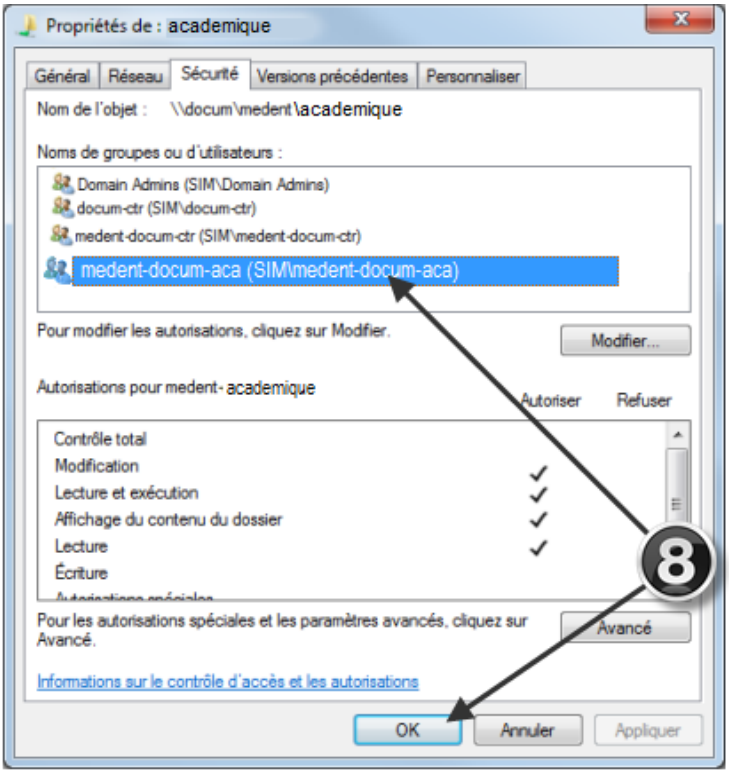
Les droits « refusés » sont prioritaires et écrasent tous les autres droits.

Ne PAS autoriser le « Contrôle total ».



7) Cliquer sur *Appliquer* pour confirmer et rester sur la page ou cliquer sur *OK* pour confirmer et fermer la page.

8) Le groupe s'affiche dans la fenêtre *Propriétés de …*, cliquer sur *OK*.



Tous les droits sont appliqués à ce dossier. Les enfants de celui-ci hériteront des mêmes droits.

Les droits hérités du parent seront marqués de crochets en grisé au lieu d'être en noir.

5.5.6 Ne pas retirer un groupe d'accès dont les droits sont hérités = NON RECOMMANDÉ

Cette manœuvre est délicate car elle exige que l'héritage soit coupé. Cette coupure entrainerait des conséquences importantes difficiles à corriger.

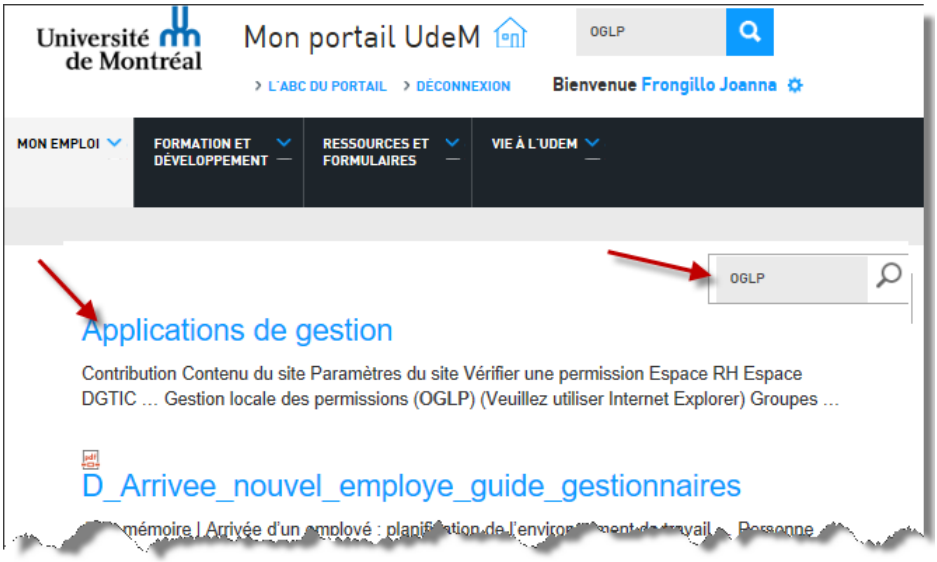
RECOMMANDATION : NE JAMAIS COUPER L'HÉRITAGE

6 Gestion des groupes par l'outil de gestion locale des permissions (OGLP)

Pour gérer les groupes, il est essentiel que le responsable s'authentifie avec son **code d'accès utilisateur** et non pas le compte ca-unité.

6.1 Accéder à l'OGLP

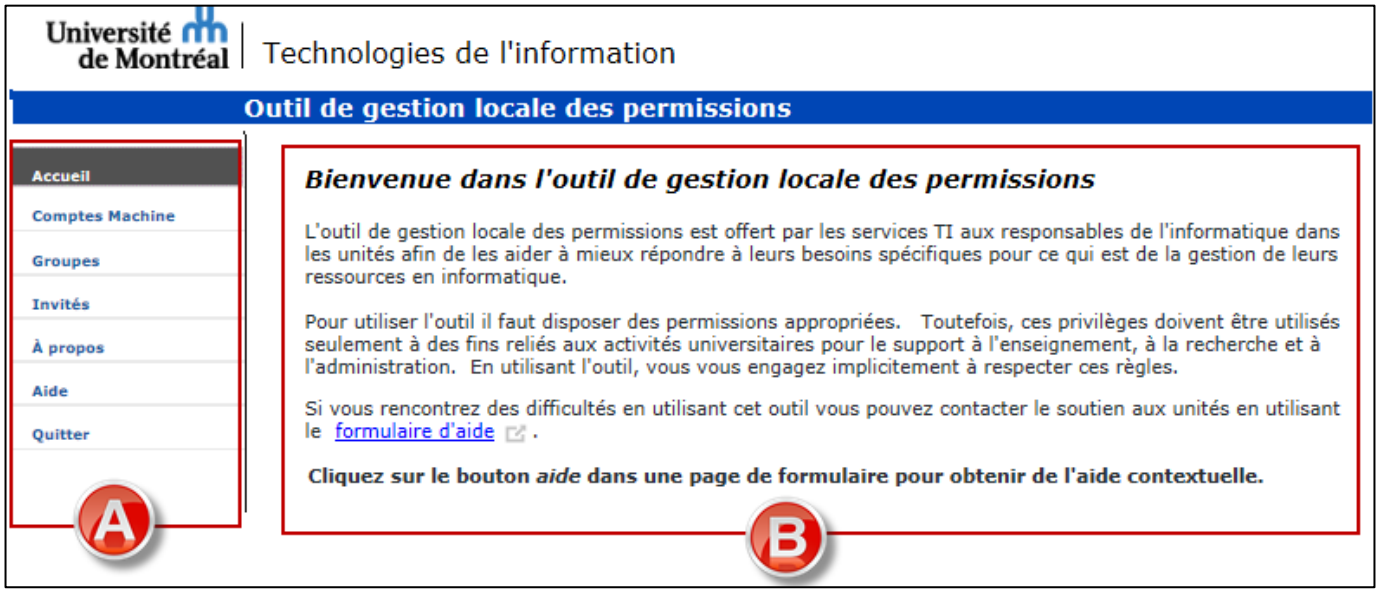
- Par le portail employé en faisant une recherche du terme OGLP.



- Par l'URL: https://www2.portail.umontreal.ca/oglp.

6.2 Naviguer dans l'OGLP

Lors de l'entrée dans l'outil, une fenêtre semblable à celle-ci apparaît :

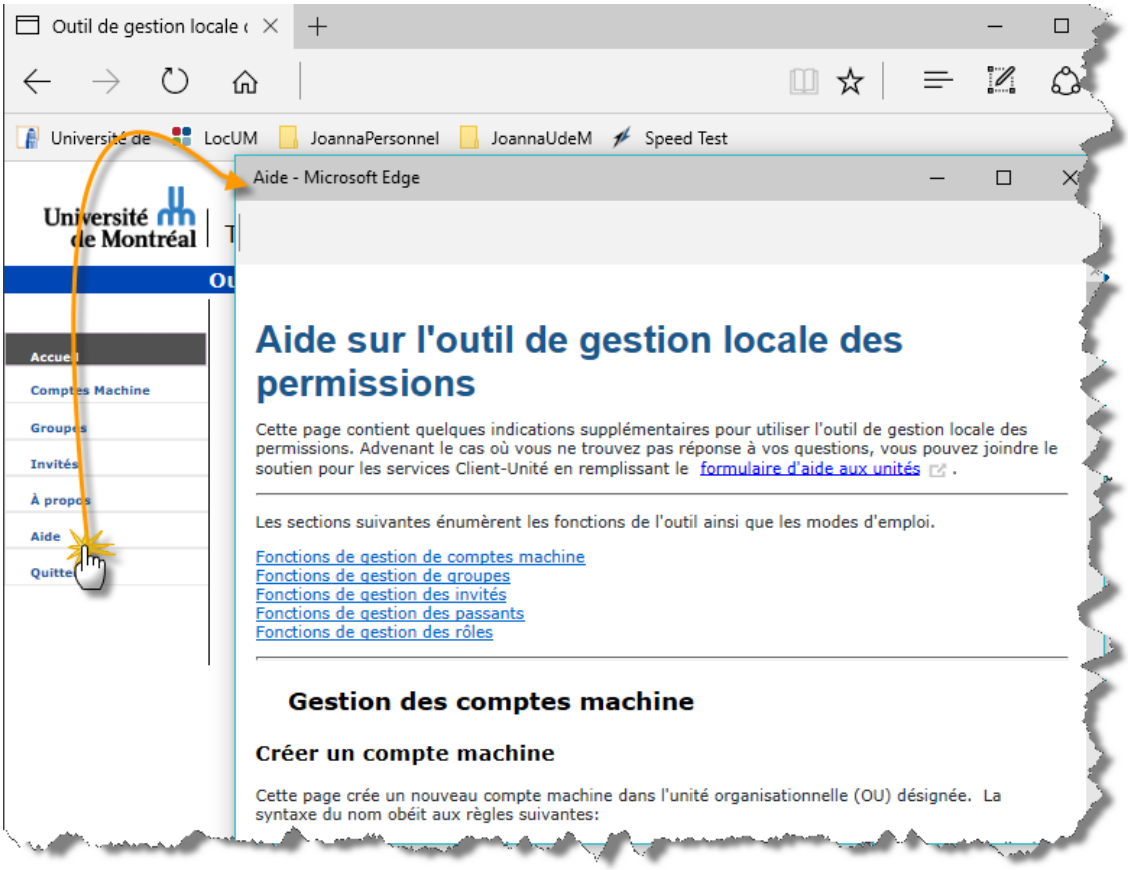


A) La partie de gauche permet la navigation parmi les options auxquelles l'utilisateur possède des droits. Dès que le curseur atteint une option, un sous-menu apparaît donnant accès à ses sous options.

B) La partie de droite permet d'obtenir les informations relatives à l'option sélectionnée dans le menu de gauche.

6.3 Accéder à l'aide en ligne

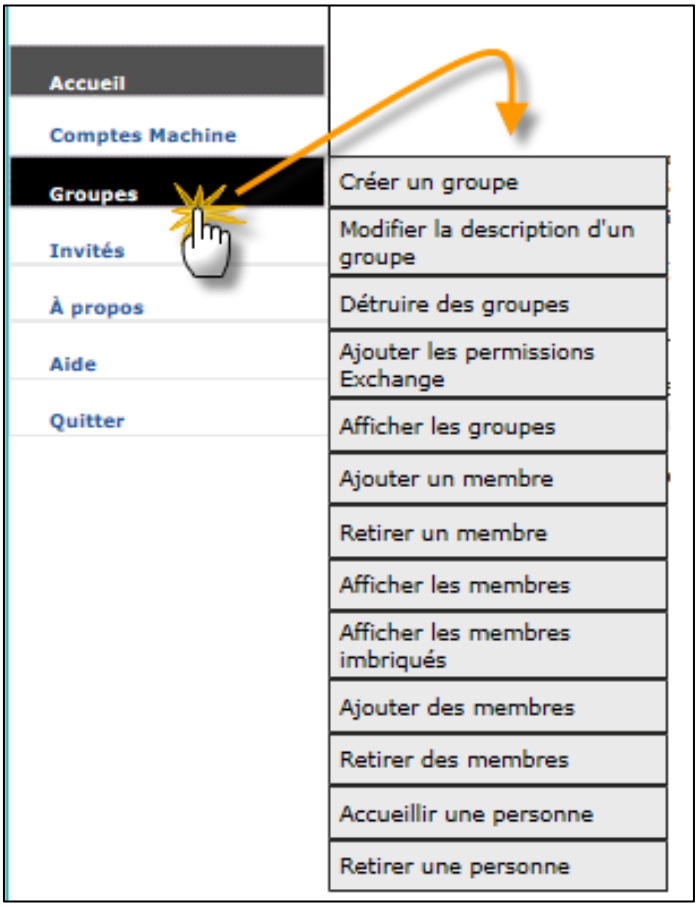
Il est facile de consulter l'option « Aide » pour obtenir toutes les informations concernant l'OGLP directement dans l'outil.



6.4 Le menu « Groupes »

Permet de :

- Créer un groupe
- Modifier la description d'un groupe
- Détruire un groupe
- Ajouter les permissions Exchange
- Afficher les groupes
- Ajouter un membre
- Retirer un membre
- Afficher les membres
- Afficher les membres imbriqués
- Ajouter des membres
- Retirer des membres
- Accueillir une personne
- Retirer une personne



6.5 Gérer le groupe principal et les groupes secondaires

Il existe deux (2) types de groupe soit le **groupe principal** et les **groupes secondaires**.

1. Le **groupe principal** – Ce groupe est créé par les TI

   Au moment de la création de l'unité, les administrateurs des TI créent le groupe principal. Par défaut les membres de ce groupe ont des accès aux ressources communes de l'unité telles que :

   - ✓ Partages de fichiers sur les serveurs institutionnels avant DocUM (Ocean, Fama, Prunier, Everest…)
   - ✓ Imprimantes
   - ✓ Dossiers publics d'Exchange
   - ✓ Toute autre ressource commune de l'unité (Wiki, Webdépôt par exemple)

   Il est possible cependant que l'unité décide de restreindre l'accès à certaines de ces ressources. Le responsable doit alors créer des groupes secondaires et ensuite demander de faire appliquer les droits d'accès aux ressources spécifiques. Le cas de figure suivant nous en donne un exemple.

   Cas de figure :

   Le responsable de l'unité xyz désire restreindre l'accès aux imprimantes en réseau à quelques membres de l'unité seulement. Il devra :

   1) Créer un groupe secondaire (nommé par exemple xyz-imprimantes) et inclure des membres ;
   2) Faire appliquer les droits d'accès du groupe sur l'imprimante par le soutien aux unités des TI (voir coordonnées au chapitre 9) ;
   3) Faire retirer le groupe principal sur l'imprimante par le soutien aux unités.

   Ainsi, seuls les membres du groupe secondaire « xyz-imprimantes » ont des droits d'impression.

Le **groupe principal** ne donne pas accès au partage de fichiers dans DocUM. Pour donner des accès à DocUM, le responsable de l'OGLP doit imbriquer le ou les groupes secondaires dans le groupe nommé ***unite-docum*** (porte d'entrée de DocUM).

Après la migration sur DocUM et à moins d'avis contraire, le **groupe principal** sera toujours appliqué par défaut sur les autres ressources (imprimantes, dossiers Exchange…)

2. Les **groupes secondaires** – Ces groupes sont créés par le responsable de l'OGLP dans l'unité.

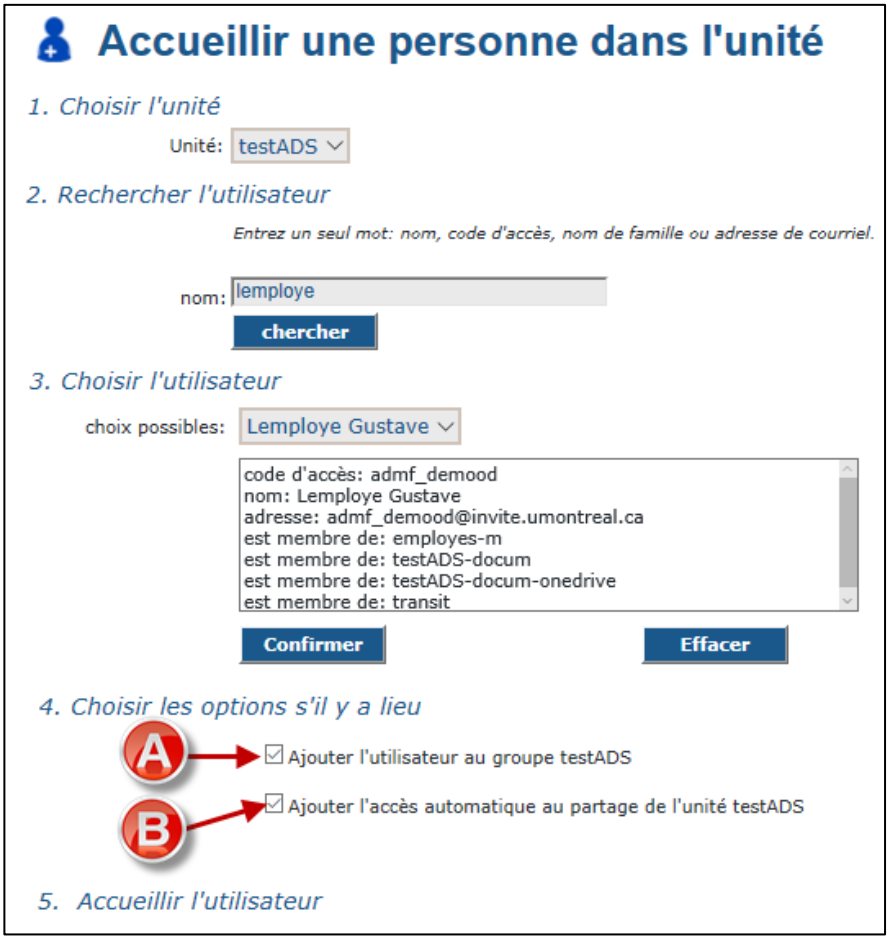
   Les groupes secondaires servent à donner des accès spécifiques à des ressources telles que :

   - Dossiers (secteurs et sous-secteurs) de l'espace DocUM ;
   - Sous-dossiers spécifiques Exchange ;
   - Restriction sur les imprimantes (cas de figure ci-haut mentionné) ;
   - Restriction sur les accès à l'espace Wiki.
   - Restriction sur toute autre ressources informatique.

6.6 Accueillir une personne dans l'unité

La fonctionnalité « Accueillir une personne dans l'unité » permet à l'utilisateur accueilli d'obtenir des accès selon les besoins de chaque unité. Elle n'est pas toujours nécessaire pour tous.

Explication des deux (2) options suivantes :



A) *Ajouter l'utilisateur au groupe « unité »*

Permet d'ajouter l'utilisateur dans le groupe principal de l'unité.

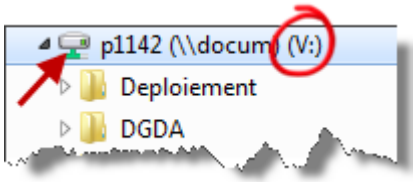
Les membres de ce groupe ont des accès aux ressources communes de l'unité. Attention car celles-ci peuvent être différentes d'une unité à l'autre. Cependant, dans la plupart des cas, il s'agit des principalement des ressources suivantes :

- ✓ Partages de fichiers sur les serveurs institutionnels avant DocUM (Ocean, Fama, Prunier, Everest…)
- ✓ Imprimantes
- ✓ Dossiers publics d'Exchange

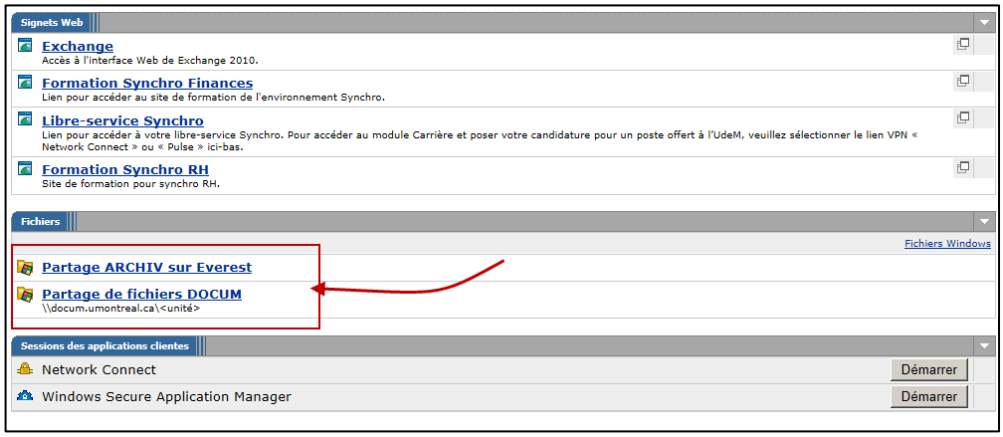
Pour permettre l'accès à l'espace de partage DocUM, l'utilisateur doit être ajouté à un groupe de secteur qui lui, est imbriqué au groupe **unité-docum**.

B) *Ajouter l'accès automatique au partage de l'unité*

Permet que l'espace de partage de l'unité (Docum, Ocean, Fama…) soit connecté automatiquement au démarrage de la session de travail sous la lettre V.



Lors d'une connexion à distance, l'espace de partage **DocUM** ou **EVEREST** est connecté automatiquement.



Cas de Jacinthe – **Invitée** au département de philosophie

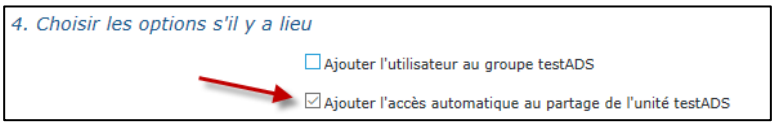
Les données de l'unité sont migrées sur DocUM et aucun groupe secondaire n'est appliqué sur les ressources communes; celles-ci sont donc accessibles aux membres du groupe principal « philo ».

Jacinthe doit pouvoir travailler à distance et accéder aux dossiers concernant l'administration sur DocUM seulement. Elle ne doit pas avoir accès aux imprimantes ni aux dossiers publics Exchange.

Dans ce cas de figure, Jacinthe ne doit pas être accueillie dans le groupe principal.

Le responsable doit :

- Créer un compte invité pour Jacinthe (*philo-jacinthe*).
- Accueillir *philo-jacinthe* en ne cochant que la case « *Ajouter l'accès automatique… »*.



  Le V: sera alors automatiquement connecté au partage de philo et la connexion VPN sera possible.

- Ajouter *philo-jacinthe* au groupe secondaire donnant des droits au dossier du secteur *Administration* (philo-docum-administration qui lui est imbriqué dans le groupe philo-docum).

La communauté « Invités » doit obligatoirement démarrer une connexion VPN pour accéder à DocUM, autant sur le campus qu'à l'extérieur. Par contre, les employés et étudiants doivent effectuer une connexion VPN que de l'extérieur.

Si Jacinthe obtenait la permission d'imprimer, elle devrait alors être ajoutée au groupe principal. Le responsable, devra l'accueillir et cocher la case « *Ajouter l'utilisateur au groupe philo »* ce qui lui donnera accès aux imprimantes.

Tout nouveau compte invité est automatiquement ajouté au groupe *unite-invites* (groupe général pour les invités).

6.6.1 Procédure

1) Au besoin, sélectionner l'unité.

2) Saisir le code d'accès ou l'adresse courriel de l'utilisateur et *chercher*. Les choix possibles s'affichent.

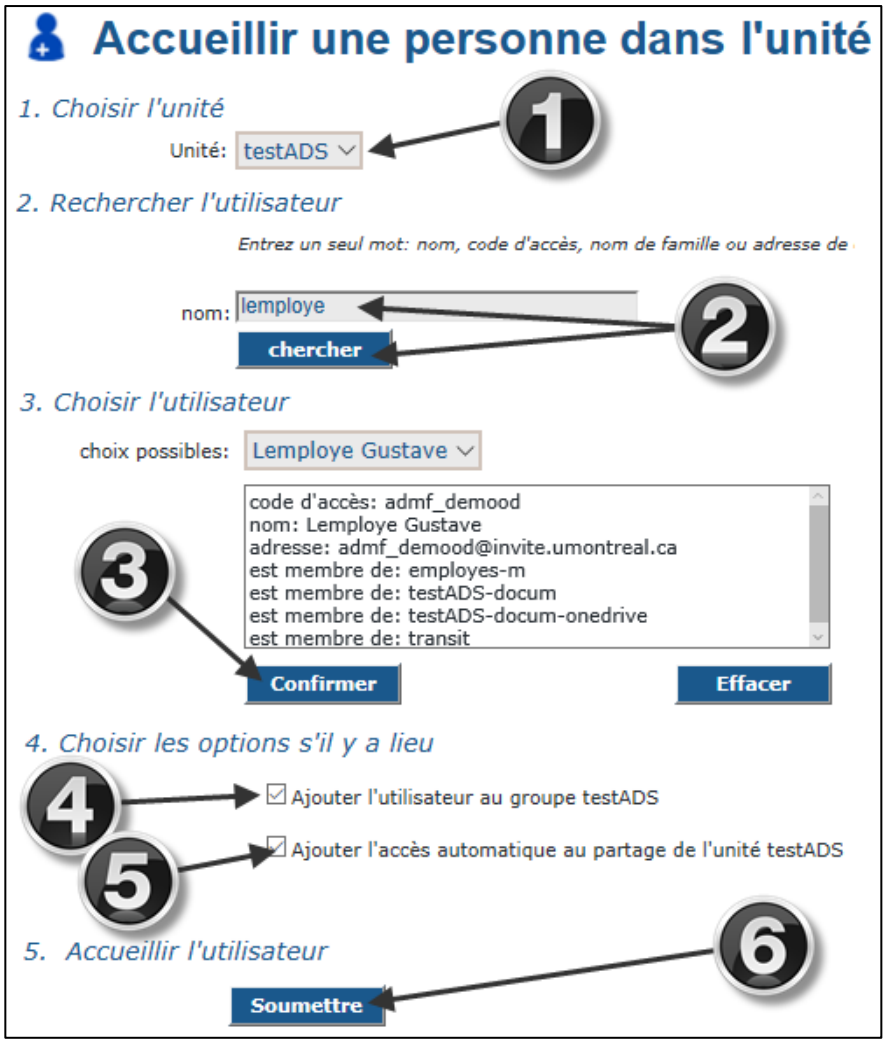
   S'il y a plusieurs choix, sélectionner la bonne personne (il pourrait y avoir plus d'une personne portant le même nom).

3) *Confirmer*.

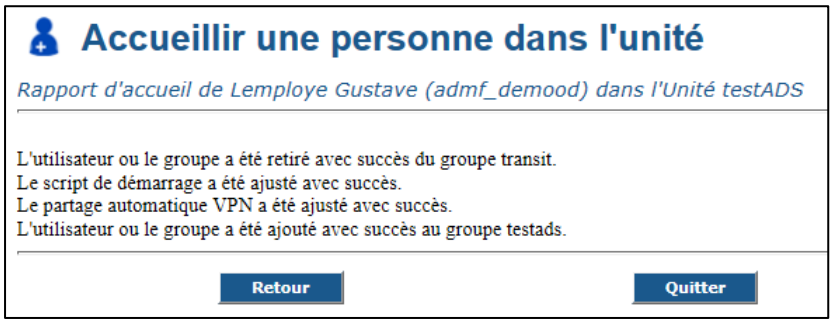
4) Seulement pour permettre à l'utilisateur d'accéder aux ressources communes, cocher la case *Ajouter l'utilisateur au groupe xxx*.

5) Pour permettre à l'utilisateur d'accéder au partage de fichiers de l'unité par le VPN, et pour que la connexion au V: soit automatique, cocher la case *Ajouter l'accès automatique au partage de l'unité xxx.*

6) *Soumettre*.



Un rapport s'affiche.



6.7 Retirer une personne de l'unité

La fonctionnalité « Retirer une personne de l'unité » permet de retirer tous les droits d'accès de l'utilisateur de l'unité.

1) Au besoin, sélectionner l'unité.

2) Saisir le code d'accès ou l'adresse courriel de l'utilisateur et chercher. Les choix possibles s'affichent.

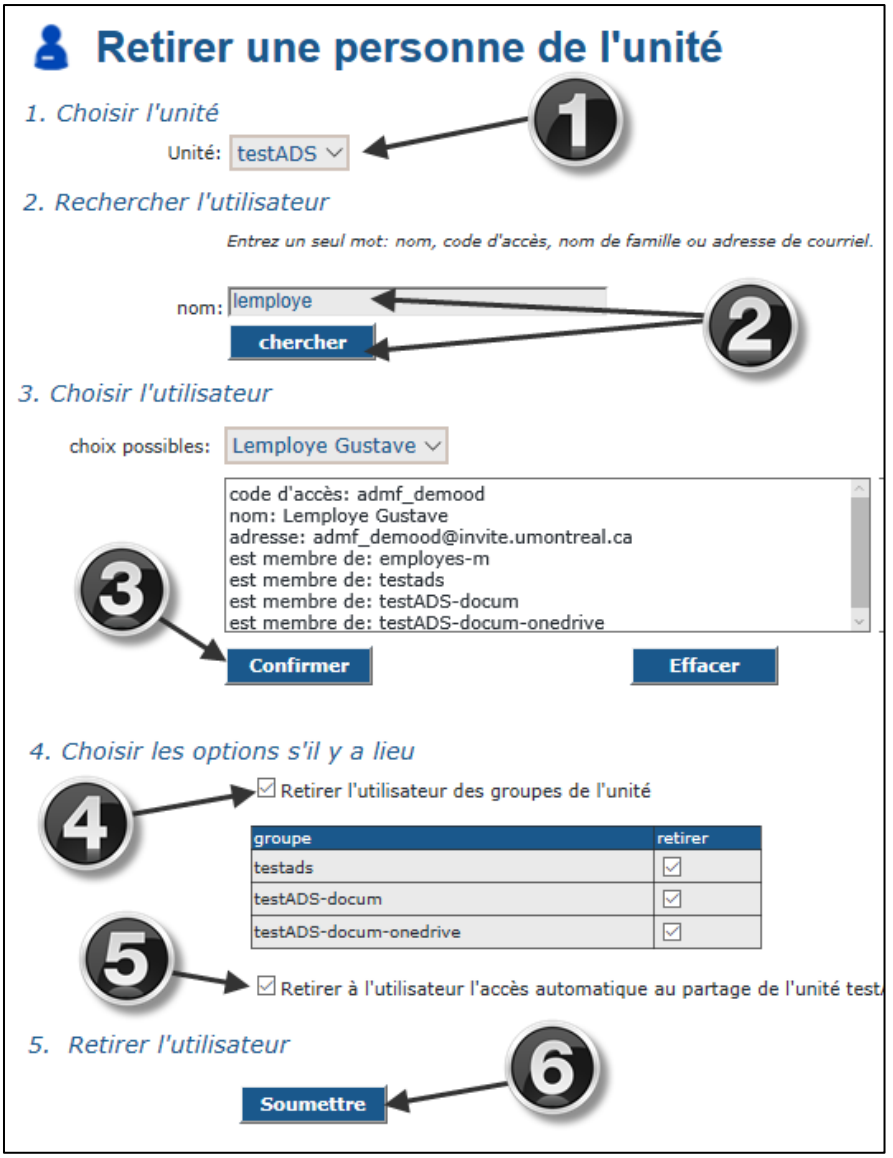
   S'il y a plusieurs choix, sélectionner la bonne personne (il pourrait y avoir plus d'une personne portant le même nom).

3) *Confirmer*.

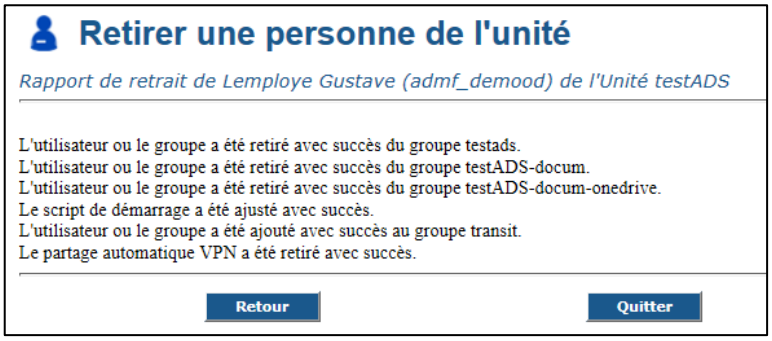
4) S'il s'agit d'un départ, s'assurer que tous les groupes soient cochés. Il est possible ici de le retirer de quelques groupes seulement.

5) S'il s'agit d'un départ, s'assurer que la case *Retirer à l'utilisateur l'accès automatique au partage de l'unité xxx* est bien cochée.

6) *Soumettre*.



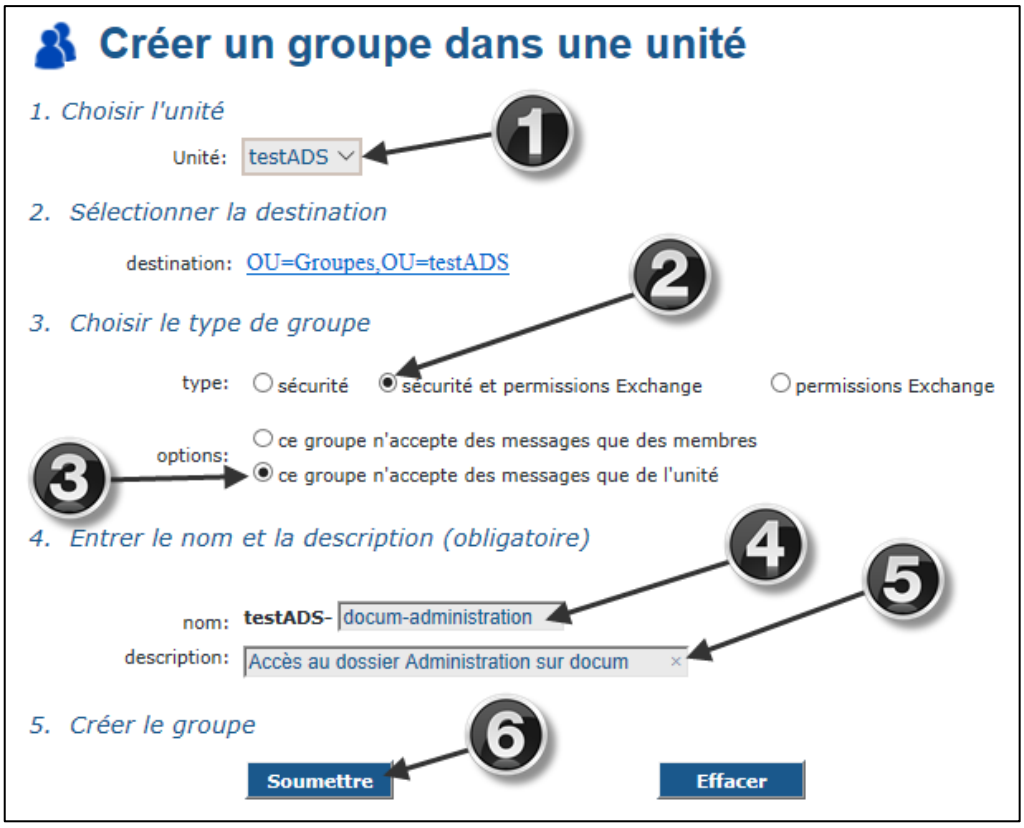
Une confirmation s'affiche.



6.8 Créer un groupe (secondaire)

1) Au besoin, sélectionner l'unité.
2) Sélectionner le type *sécurité et permissions Exchange*.

Créer toujours des groupes de type *sécurité et permissions Exchange* pour permettre l'envoi de courriel.



3) Choisir l'option « *ce groupe n'accepte des messages que de l'unité* ».
4) Saisir le complément du nom du groupe **en minuscules** (voir suggestions au chapitre 6.8.2 à la page 33).
5) Saisir une **description explicite**.

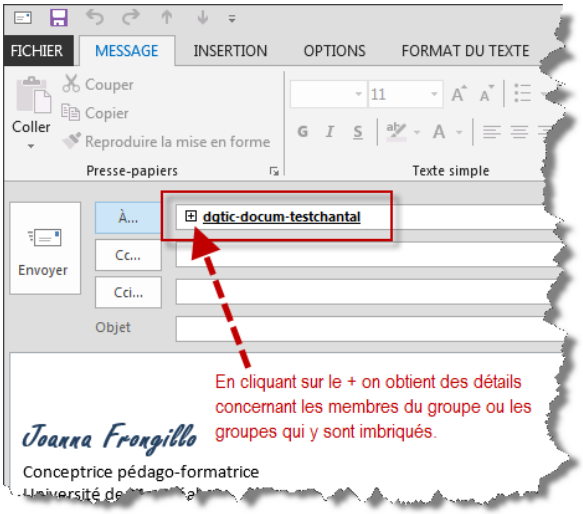
La description permet de garder une trace de l'utilité du groupe. Celle-ci s'affichera lorsque l'utilisateur demandera une liste des groupes.

6) *Soumettre*.

Un rapport s'affiche.

6.8.1 Utilisation d'une liste de distribution

Lorsqu'un groupe est créé avec le type « Permissions Exchange », il est alors possible que ses membres puissent s'écrire entre eux ou que les membres de l'unité puissent écrire au groupe (selon l'option choisie).



Même s'il s'agit d'un groupe ne contenant qu'une seule personne, il est important de choisir le type « Permissions Exchange », puisque celui-ci sera sans doute imbriqué à un autre groupe où cette fonctionnalité sera également choisie.

6.8.2 Suggestions pour nommer les groupes

- Afin de bien identifier l'utilité de chaque groupe, il est fortement recommandé d'utiliser les types suivants :
  - ***docum*** dans le nom des groupes donnant accès à DocUM ;
  - ***imp*** dans le nom des groupes donnant accès aux imprimantes ;
  - ***bal*** dans le nom des groupes donnant accès aux boîtes aux lettres partagées ;
  - ***wiki*** dans le nom des groupes donnant accès au wiki.
- Utiliser toujours les minuscules. Certaines technologies sont sensibles à la casse (Linux). Il sera donc plus facile si la minuscule est utilisée pour nommer tous les groupes.
- Le nom des groupes est limité à 50 caractères.
- Éviter les signes diacritiques (accents et ponctuation) et les caractères spéciaux.
- Éviter d''utiliser le caractère « soulignement », utiliser plutôt le tiret au besoin. Ceci évite la confusion lorsqu'un groupe détient la permission Exchange. Dans une adresse courriel le lien hypertexte cache le caractère de soulignement et nous fait croire qu'il s'agit d'un espace.
- Utiliser le masculin et le singulier.
- Utiliser les types et suffixes suivants au besoin :

Type	Groupe pour identifier
docum	L'accès aux dossiers de DocUM
imp	L'accès à une ou plusieurs imprimantes
bal	L'accès à une BAL partagée
wiki	L'accès au wiki
fct	Une fonction
Pro	Un processus, un projet ou un programme
com	Un comité
srv	Un serveur
fax	Un fax
cal	Les accès à un calendrier
ctc	Les accès à des contacts
bd	Les accès à une base de données
aut	La session d'automne
ete	La session d'été
hiv	La session d'hiver

Suffixe	Groupe pour permission en
ecr	Écriture
lec	Lecture
mod	Modification
ctr	Contrôle total

Exemples de nom de groupe	
unite-type-secteur	scinf-docum-direction
unite-type-titre	scinf-imp-e624
unite-type	scinf-wiki
unite-type-secteur-type	scinf-docum-acad-ete
unite-type-secteur-permission	scinf-docum-acad-lec

Il est judicieux d'utiliser le type de groupe toujours au même endroit dans le nom des groupes (soit tout de suite après l'acronyme de l'unité). Ainsi tous les groupes portant le même type seront regroupés ensemble lors de la production d'un rapport. Par exemple, l'utilisation du filtre dans Excel permettra d'afficher les groupes de même type.

6.8.3 Possibilité de faire créer des groupes et d'insérer des membres en lot

Pour plus de 20 groupes, il existe une possibilité de faire créer des groupes en lot (incluant des membres ou des groupes imbriqués) par le Soutien aux unités des TI. Il faut fournir un seul fichier Excel pour les deux (2) procédures détaillées plus bas.

A) Procédure pour la création de nouveaux groupes - les données doivent être saisies de la façon suivante :

Colonne 1 : Nom du groupe à créer **en minuscules, sans accent ni espace** – ce nom doit se répéter autant de fois qu'il y a de membres à ajouter ou de groupes à imbriquer.

Colonne 2 : Le ou les codes d'accès des membres à ajouter et le ou les groupes à imbriquer.

Colonne 3 : Description du groupe – seulement sur la première ligne du nouveau groupe. **Il est obligatoire de saisir une description. Celle-ci permet de garder une trace de son utilisation**.

Colonne 4 : Saisir « x » pour permettre l'utilisation d'une liste de distribution (permission Exchange) où les membres pourront être rejoints par tous les membres de l'unité par courriel – seulement sur la première ligne d'un nouveau groupe.

B) Procédure pour ajouter des membres ou imbriquer des groupes dans un groupe déjà existant - les données doivent être saisies de la façon suivante :

Colonne 1 : Nom du groupe déjà existant – ce nom doit se répéter autant de fois qu'il y a de membres à ajouter ou de groupes à imbriquer.

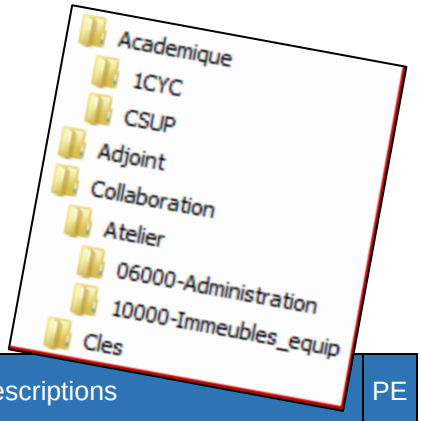
Colonne 2 : Le ou les codes d'accès des membres à ajouter et le ou les groupes à imbriquer.

Colonne 3 et 4 : Aucune description n'est nécessaire puisque le groupe est déjà existant.

- L'ordre est très important. La création d'un nouveau groupe doit apparaitre dans le fichier Excel avant d'y ajouter des membres ou d'y imbriquer des groupes.
- Les codes d'accès des personnes doivent être valides et sans erreur.
- Il n'est pas possible d'utiliser cette procédure pour ajouter ou modifier une description ou pour permettre qu'un groupe obtienne une permission Exchange (colonnes 3 et 4) pour un groupe existant. Les 2 dernières colonnes ne servent qu'au moment de la création d'un nouveau groupe.
- **Réviser les données minutieusement afin que le fichier ne comporte aucune erreur. Les données sont traitées par un script et il pourrait être très long de corriger les erreurs générées.**

Voir un exemple d'un fichier Excel à la page suivante.

Dans l'exemple suivant, certaines lignes ont été placées en gras pour aider à la lecture, il n'est pas nécessaire de reproduire ce format.



Groupes	Membres (code d'accès ou groupes)	Descriptions	PE
psy-docum-1cyc	Caronji	Accès en modification au secteur 1ER CYC sur docum	x
psy-docum-csup	vinetgi	Accès en modification su secteur CSUP sur docum	x
psy-docum-csup	bouclairs		
psy-docum-academique	psy-docum-1cyc	Accès aux secteurs ACADÉMIQUE sur docum	x
psy-docum-academique	psy-docum-csup		
psy-docum-adjoint	frongilj	Accès en modification au secteur ADJOINT sur docum	x
psy-docum-adjoint	josephc		
psy-docum-adjoint-lec	campeaus	Accès en lecture au secteur ADJOINT sur docum	x
psy-docum-adjoint-lec	leducjo		
psy-docum-adjoint-lec	denisna		
psy-docum-atelier	parentju	Accès en modification au secteur ATELIER sur docum	x
psy-docum-atelier	Caronpa		
psy-docum-cles	bourhista		
psy-docum-collaboration	psy-docum-atelier	Accès aux secteurs COLLABORATION sur docum	x
psy-docum-collaboration	psy-docum-cles		
psy-docum	psy-docum-academique	Comme le groupe psy-docum est déjà existant, inutile de mettre une description et une mention PE.	
psy-docum	psy-docum-adjoint*		
psy-docum	psy-docum-adjoint-lec*		
psy-docum	psy-docum-collaboration		

* Il est nécessaire ici d'imbriquer le groupe *psy-docum-adjoint et psy-docum-adjoint-lec* au groupe *psy-docum* puisqu'il n'existe pas de groupe regroupant les deux sous-groupes.

6.9 Ajouter un membre à des groupes

1) Au besoin, sélectionner l'unité.

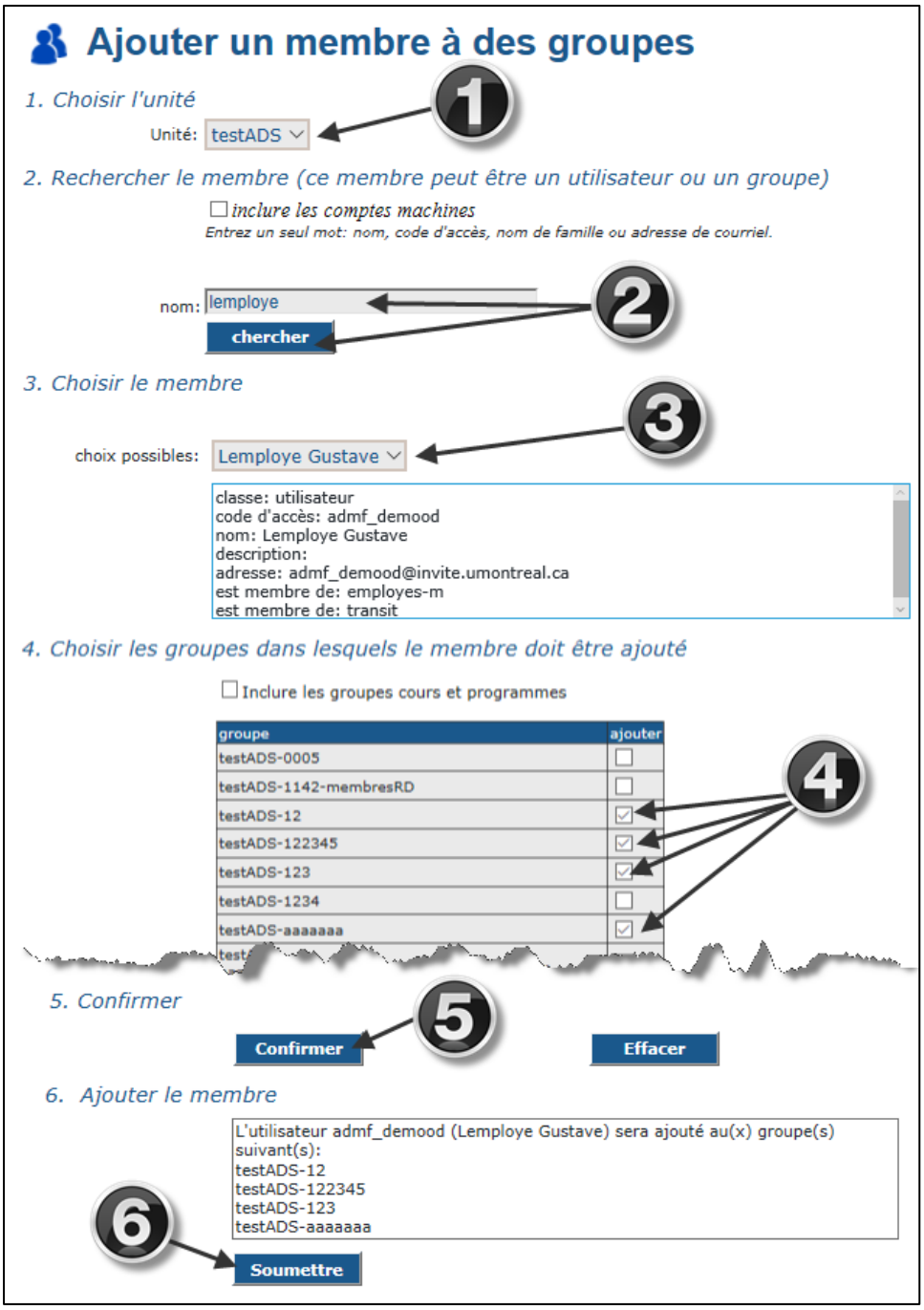
2) Saisir le code d'accès ou l'adresse courriel de l'utilisateur et *chercher*.

   Les choix possibles s'affichent.

3) S'il y a plusieurs choix, sélectionner la bonne personne (il pourrait y avoir plus d'une personne portant le même nom).

4) Cocher le ou les groupes où l'utilisateur sera ajouté.

5) *Confirmer*.



Un rapport s'affiche.

6.10 Ajouter un ou plusieurs membres à un ou plusieurs groupes

Par le menu *Groupes*, accéder à l'option *Ajouter des membres.*

1) Au besoin, sélectionner l'unité.
2) Sélectionner le ou les groupes désirés.
3) Saisir le code d'accès ou l'adresse courriel de l'utilisateur et chercher.

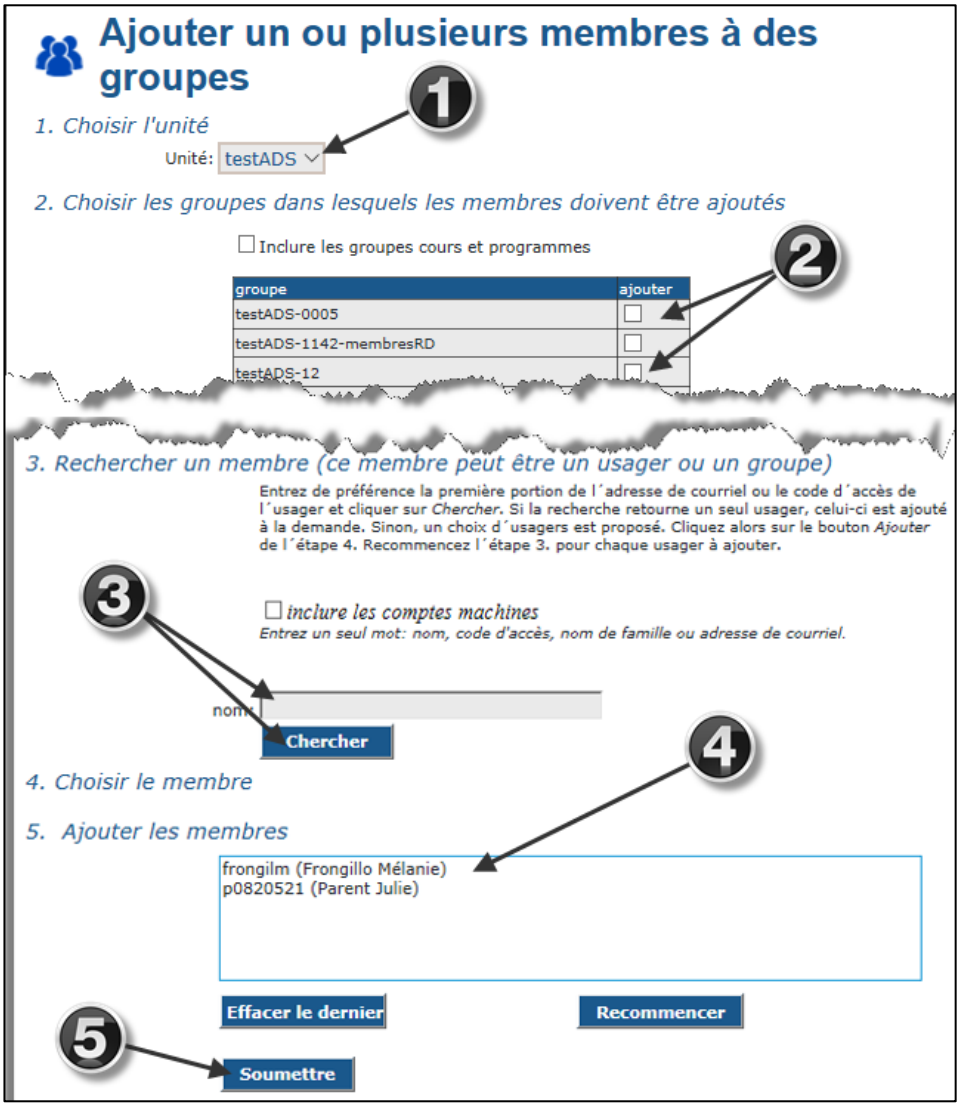
   S'il existe plus d'un choix, sélectionner l'utilisateur dont les renseignements correspondent à la personne désirée.

Il est également possible d'ajouter un ou plusieurs groupes à cette étape (ceux-ci seront imbriqués).

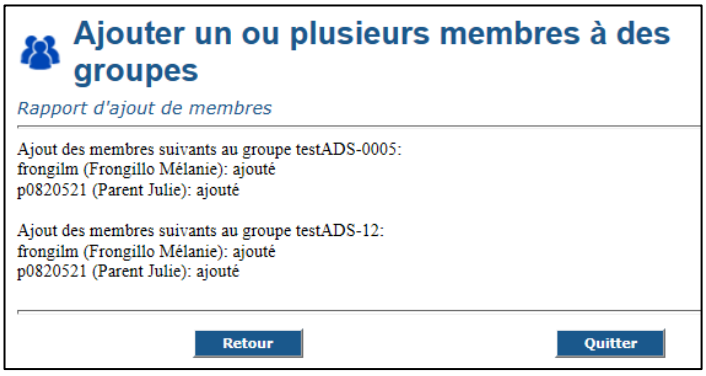
4) *Ajouter*. L'utilisateur s'affiche.

   Pour ajouter d'autres membres, refaire les étapes à partir du point 2.

5) Une fois tous les membres ajoutés, *Soumettre*.



Un rapport s'affiche.



6.11 Retirer un ou plusieurs membres d'un groupe

Par le menu *Groupes*, accéder à l'option *Retirer un ou plusieurs membres d'un groupe*.

1) Saisir le nom du groupe (en tout ou en partie) et *Chercher*.
2) S'il existe plus d'un choix, sélectionner le groupe désiré.
3) Cocher le ou les membres à retirer.
4) *Confirmer*. Le ou les membres retirés s'affichent.
5) *Soumettre*.

Un rapport s'affiche.

6.12 Afficher tous les membres de tous les groupes

Par le menu *Groupes*, accéder à l'option *Afficher les membres*

1) Ne rien indiquer dans la zone du suffixe et *Chercher*.
2) Cocher la case *Afficher tous les groupes*.
3) Sélectionner le tri.
4) *Soumettre*.

Un rapport s'affiche.

6.13 Afficher la liste des groupes

Par le menu *Groupes*, accéder à l'option *Afficher les groupes de l'unité*. Sélectionner l'option de tri et *Soumettre*. La liste des groupes de l'unité s'affiche.

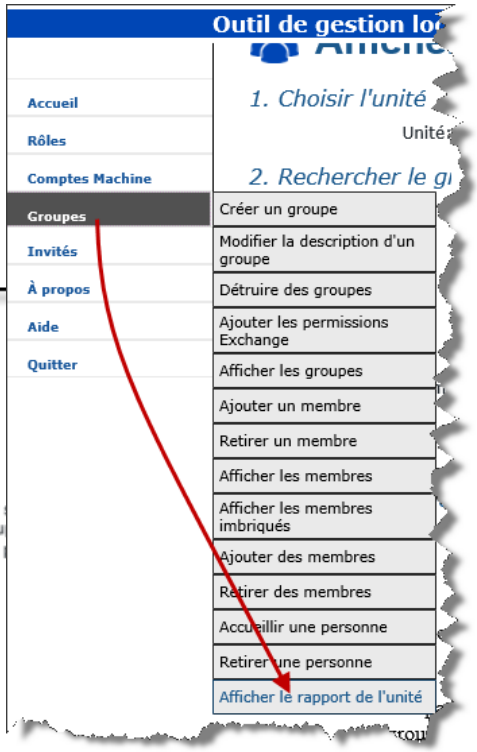
6.14 Afficher la liste des membres d'un groupe

Par le menu *Groupes*, accéder à l'option *Afficher tous les membres*.

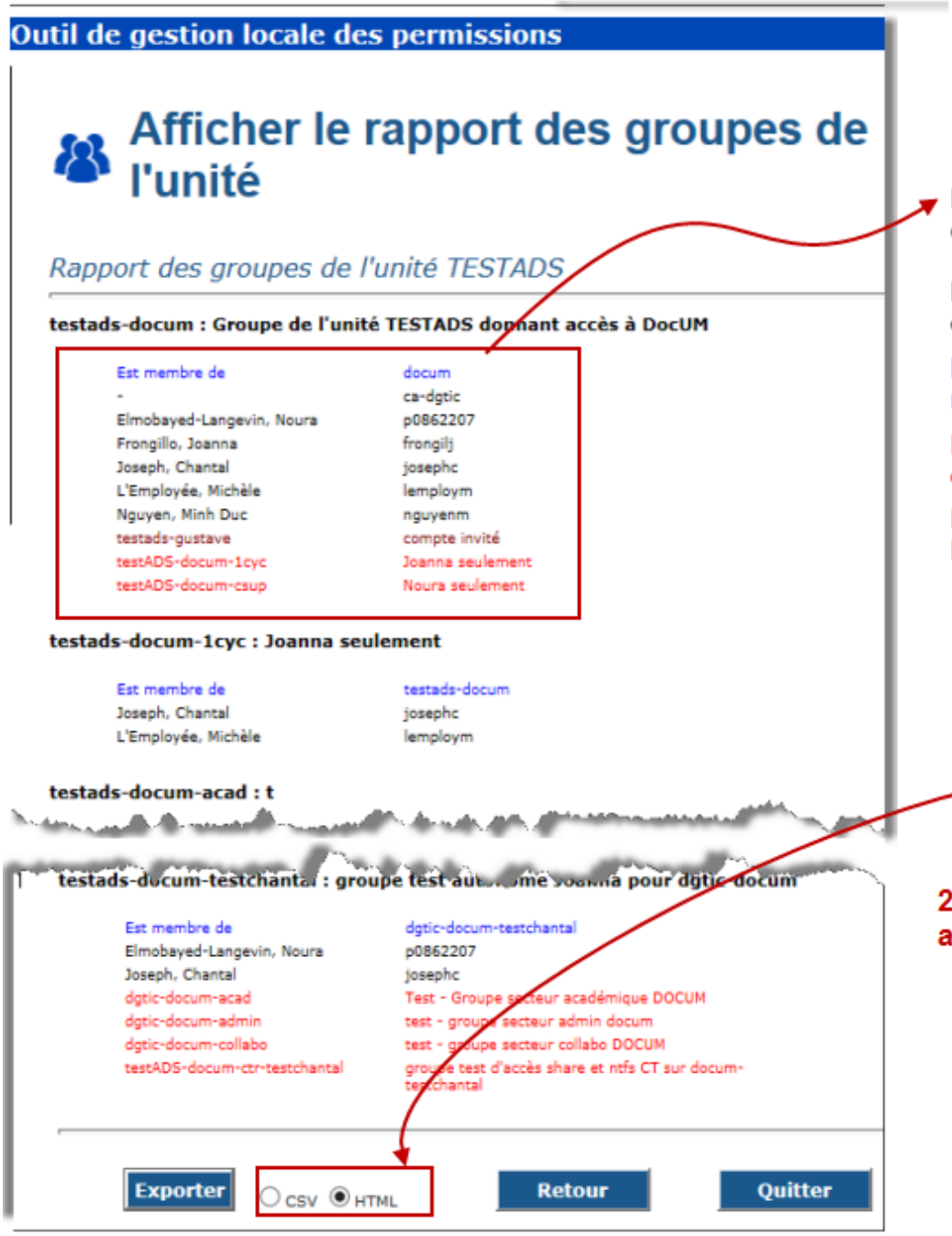
1) Saisir le nom du groupe (en tout ou en partie) et *Chercher*.
2) S'il existe plus d'un choix, sélectionner le groupe désiré.
3) Choisir l'option de tri.
4) *Soumettre*.
   La liste des membres du groupe s'affiche.

6.15 Afficher le rapport de l'unité

Les options du rapport des groupes de l'unité ont été modifiées dans le but d'aider les unités ayant des groupes qui contiennent beaucoup d'éléments. Il est possible de choisir le mode de recherche (normal ou grands groupes).



Lorsque l'option *Afficher tous les groupes* est cochée, ne rien spécifier dans la zone *Groupe.* Si cette option est décochée, saisir le nom du groupe désiré dans la zone *Groupe*.



Dans le rapport, les informations de couleur :

Noir : indique le nom et le code d'accès des membres

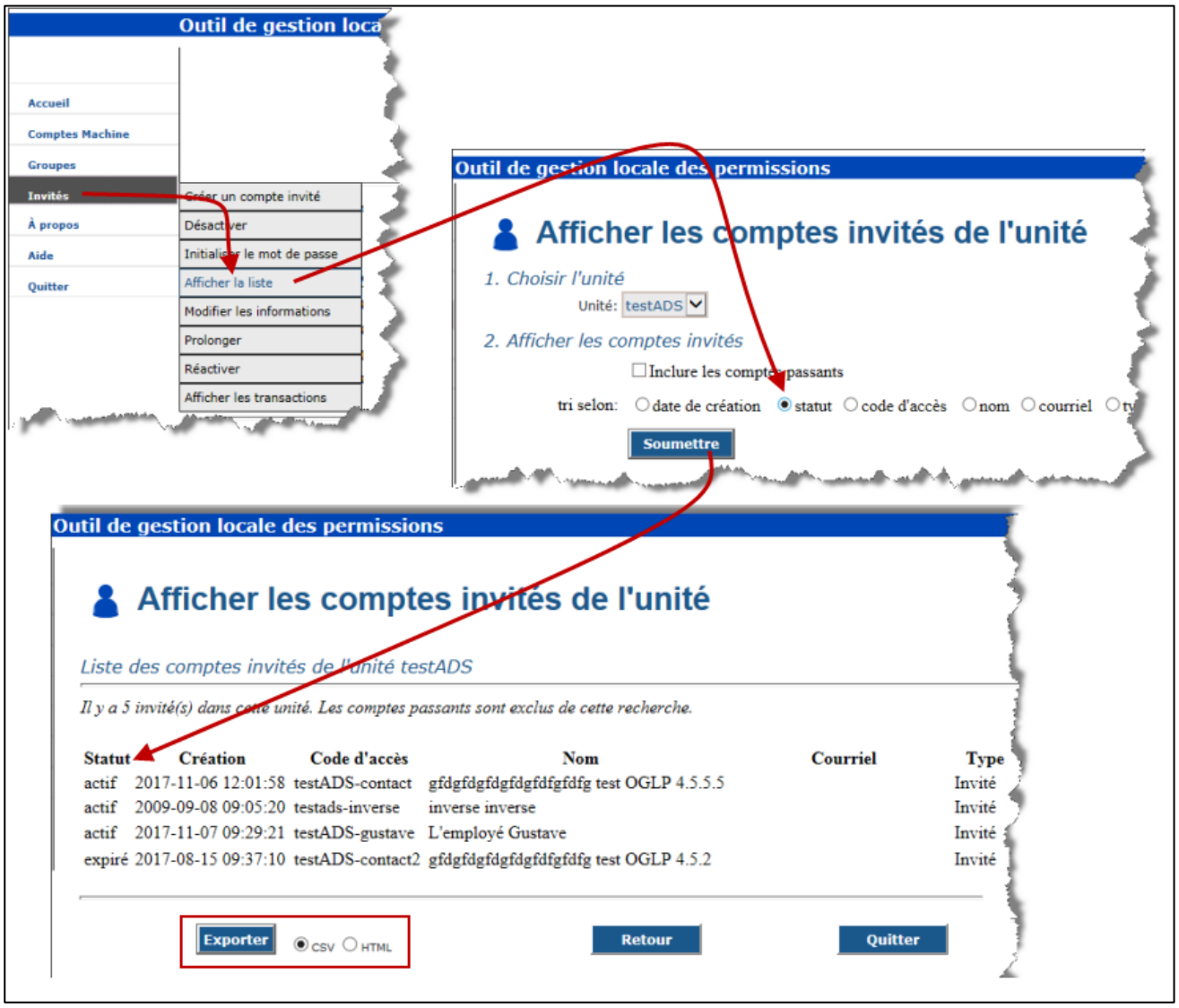
Bleu : indique que le groupe est membre d'un autre groupe

Rouge : indique le nom et la description des groupes imbriqués

Marron : indique le code d'accès et le type des comptes invités

2 choix de format possibles avant d'exporter

6.16 Afficher la liste des comptes invités par statut (nouveauté)



6.17 Détruire un groupe

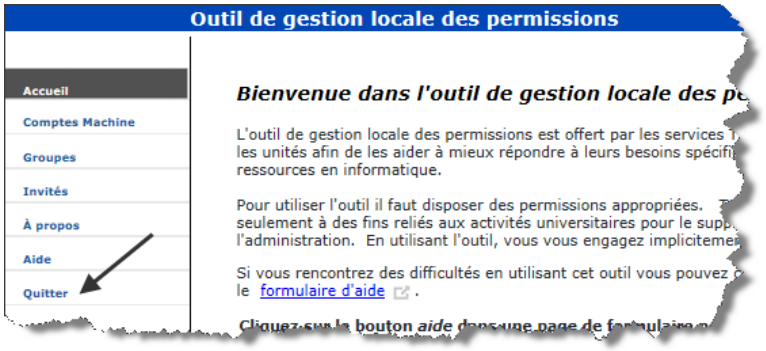
Avant de détruire un groupe, le responsable doit s'assurer qu'il n'est pas utilisé pour donner des accès sur un ou plusieurs ressources. Celui-ci doit également être vide; il faut donc retirer tous les membres du groupe avant de pouvoir le détruire.

Par le menu *Groupes*, sélectionner l'option *Détruire des groupes*.

1) Saisir le nom du groupe (en tout ou en partie) et Chercher.
2) Cocher la case *Détruire* vis-à-vis le groupe ou les groupes à détruire.
3) *Confirmer*. Le nom du ou des groupes à détruire s'affichent.
4) *Soumettre*.
   Le rapport de destruction s'affiche.

6.18 Quitter l'OGLP

Quitter l'OGLP en cliquant sur le menu *Quitter* dans la partie de gauche de la fenêtre.



7 Une structure DocUM bien montée – une gestion facile

Une fois que la structure DocUM est bien montée et que l'accès à ses dossiers est contrôlé par l'appartenance ou non à un groupe, les arrivées et départs d'employés se font rapidement, efficacement et de façon sécuritaire. La personne responsable devra porter les actions adéquates selon les besoins de l'unité par **l'OGLP seulement.**

Aucune action ne sera nécessaire quant à l'application des permissions sur la structure.

7.1 Actions à poser lors de l'arrivée d'un employé dans l'unité

7.1.1 Employé régulier

- Accueillir la personne dans le groupe principal (au besoin) et lui donner les droits au script de démarrage.
- Ajouter la personne aux groupes secondaires auxquels elle doit avoir des droits d'accès.

Attention, souvent les unités personnalisent les accès aux différentes ressources communes. Soyez vigilants !

7.1.2 Invité

- Créer le compte-invité.
- Déterminer si l'invité doit avoir les mêmes permissions que le groupe principal et si oui, l'accueillir dans ce groupe.
- Déterminer si l'invité doit avoir des droits au script de démarrage (droit sur la connexion VPN), si oui cocher la case appropriée dans « Accueillir une personne ».

7.2 Actions à poser lors du départ d'un employé dans l'unité

Lors du départ d'un employé dans l'unité, il suffira simplement de « **Retirer une personne** » et cocher tous les groupes auxquels celle-ci avait des droits.

Le fait d'ajouter le code d'accès du nouvel employé dans les groupes de l'unité ne lui enlève pas les accès de son ancienne unité. Il est de la responsabilité de l'ancienne unité de retirer les droits lors d'un départ.

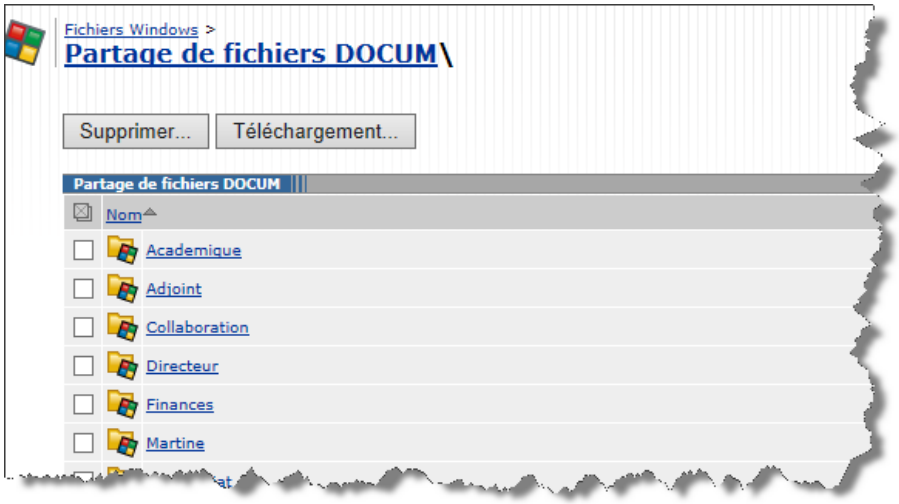
8 Accès à DocUM pour les invités

Une fois la permission adéquate (Script de démarrage) attribuée dans l'OGLP, pour accéder aux fichiers déposés dans DocUM, les invités doivent obligatoirement :

Effectuer une connexion VPN (voir détails au point 8.1 concernant la configuration du VPN). La fenêtre suivante s'affiche :

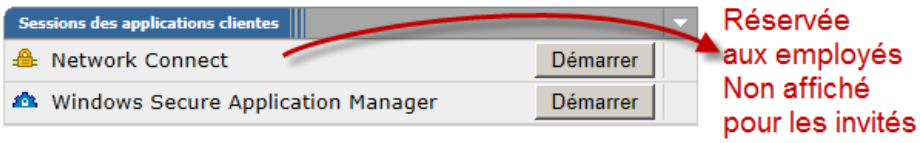
A) Section fichiers

Permet d'afficher les fichiers en mode de téléchargement.



B) Démarrer **WSAM** (plate-forme Windows) ou **JSAM** (plate-forme mac)
Permet d'ouvrir le tunnel privé vers DocUM et effectuer une connexion à DocUM de façon manuelle (voir chapitre 8.2).

Les invités ne peuvent pas effectuer un Network Connect; celle-ci est réservée aux employés seulement. Cette option n'apparaît donc pas pour les invités.



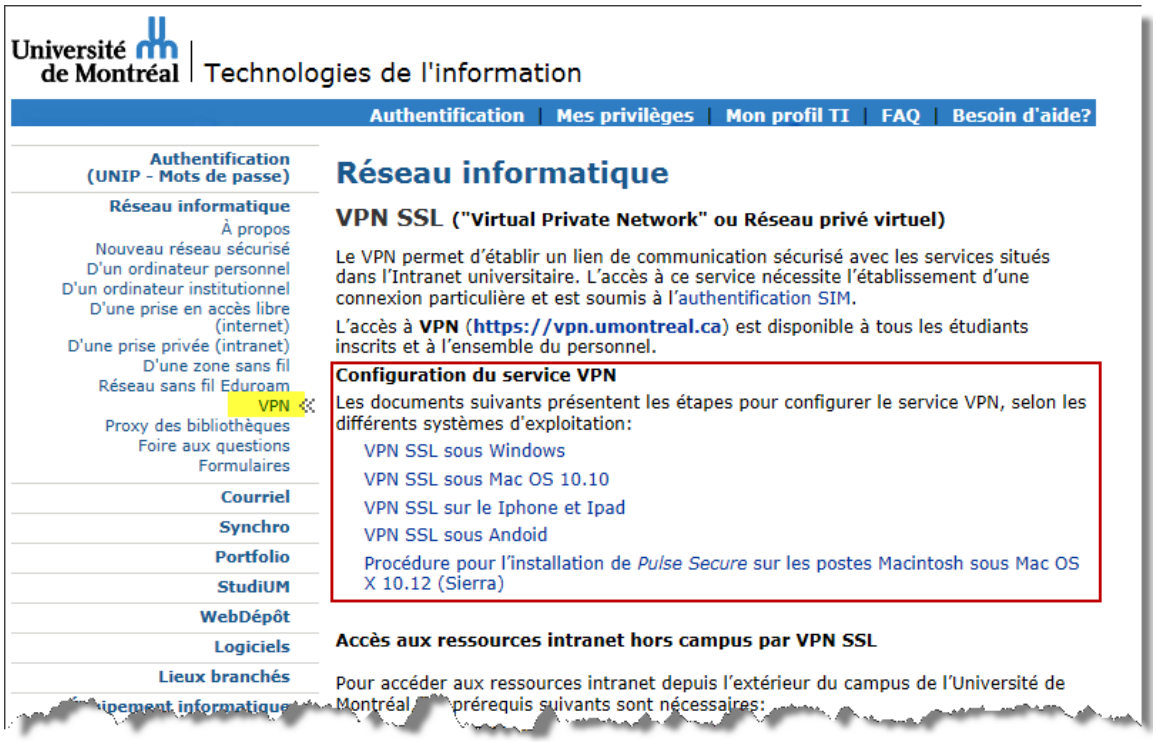
Pour les accès au réseau, les invités font partie d'une communauté distincte, leurs accès ne sont donc pas les mêmes que pour la communauté des employés. C'est pourquoi une connexion VPN est indispensable (certaines exceptions sont possibles pour le moment).

Le groupe « unité-docum » donne accès à DocUM par le VPN. Tout groupe et membre imbriqué dans le groupe « unité-docum » (y compris les comptes invités) y aura accès.

8.1 Procédure pour configurer un VPN

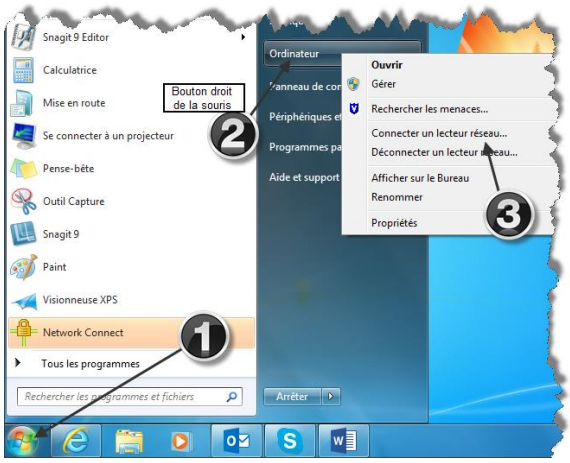
Consulter le site des TI pour obtenir toutes les procédures de configuration pour effectuer une connexion VPN.

http://www.ti.umontreal.ca/reseau/vpn.html



8.2 Procédure pour effectuer une connexion à DocUM de façon manuelle

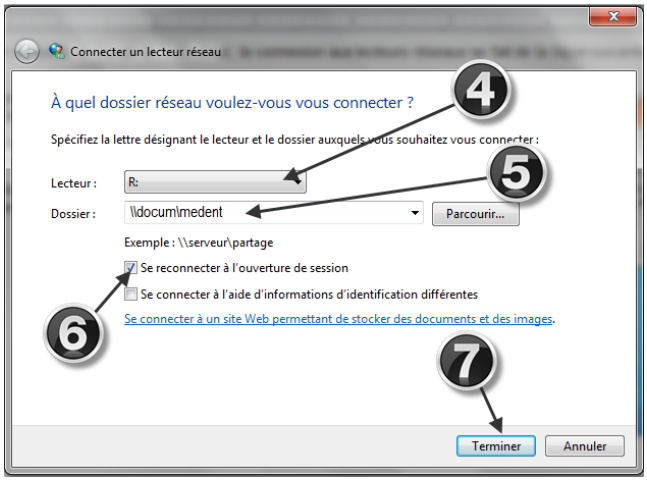
Une fois la connexion VPN établie,



1) À partir du Bureau, cliquer sur le menu *Démarrer*.
2) Cliquer (avec le bouton droit – Menu contextuel) sur *Ordinateur*.
3) Cliquer sur *Connecter un lecteur réseau*.

Note Cette procédure est valide pour tous dans le cas où le lecteur V n'est pas connecté automatiquement.

La fenêtre suivant s'affiche :



4) Choisir une lettre disponible. (Le V est réservé lors d'une connexion automatique par le script de démarrage).
5) Indiquer le nom du serveur et celui du partage en respectant le format suivant \\DocUM*Unité* (Unité = acronyme de l'unité).

Note Un invité devra saisir le lien au complet.

6) Cocher la case *Se reconnecter à l'ouverture de session* au besoin.
7) *Terminer*.

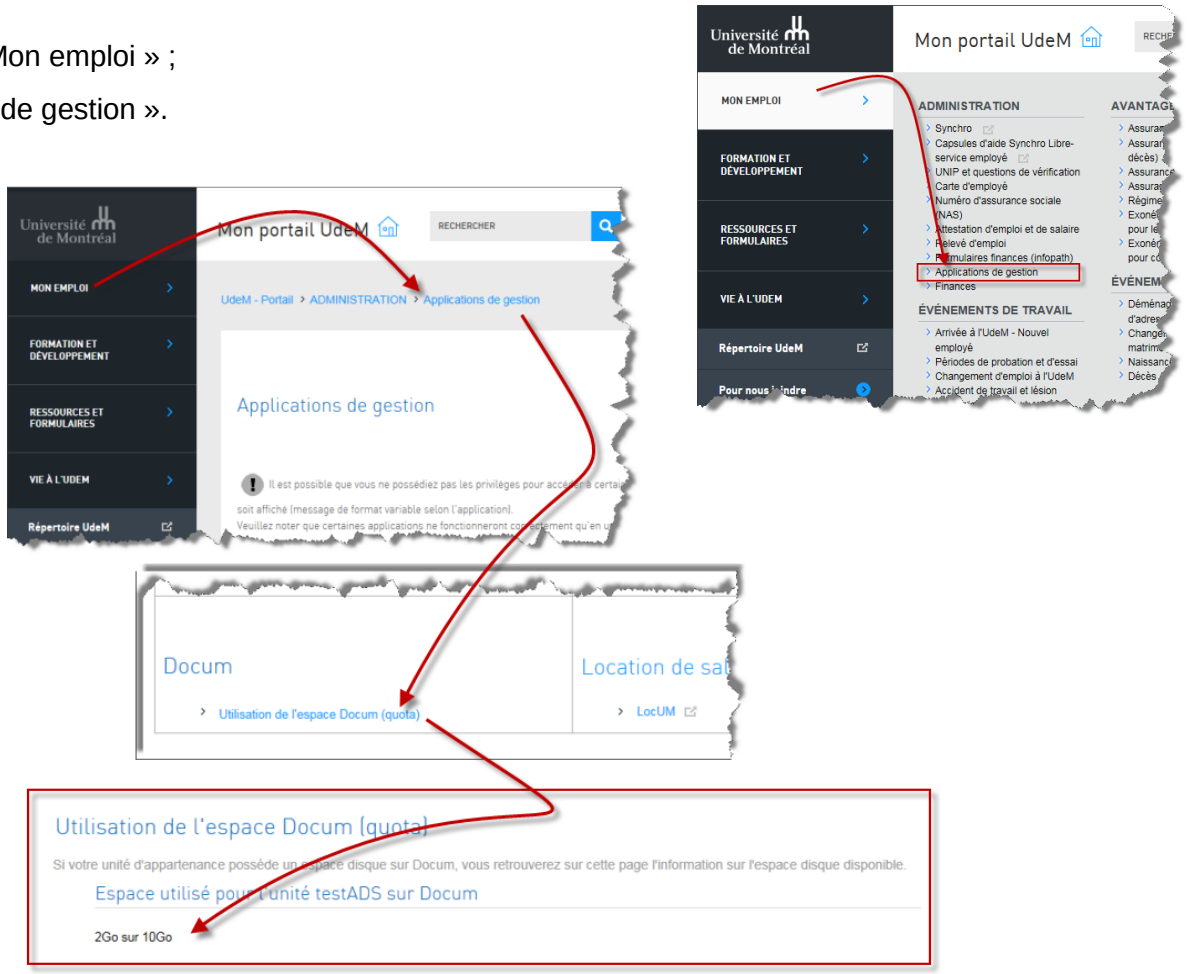
9 Consulter le quota de l'unité

Lorsque les données de l'unité sont migrées dans DocUM, il est possible de consulter le quota utilisé par portail employé.

L'espace utilisé, indiqué dans le portail, inclut les copies de fichiers pour la restauration des versions précédentes.

1. Cliquer sur « Mon emploi » ;
2. « Applications de gestion ».

Les informations se trouvent en bas de la page.



10 Obtenir de l'aide, s'inscrire à une formation et s'abonner aux avis de maintenance des TI

La personne responsable de la gestion de DocUM dans l'unité peut obtenir de l'aide en :

- Remplissant le formulaire d'aide aux unités : www.ti.umontreal.ca/secure/Formulaire_aide_unites/formulaire_aide_responsables_unites.html *(Si vous avez des problèmes d'accès à ce formulaire, téléphonez au 1740)*.
- Téléphonant au poste : 1740 entre 8 h et 12 h et 13 h 30 à 16 h 30.
- S'inscrivant à la formation « Gestion des accès dans DocUM » d'une durée de 3 heures. Celle-ci est strictement réservée aux employés qui ont un rôle à jouer dans la gestion des permissions d'accès dans DocUM. Pour s'inscrire, envoyer un courriel à inscription-formation-ca-1142@ti.umontreal.ca.
- S'abonnant à http://www.listes.umontreal.ca/wws/info/ti-imprevus afin de recevoir les avis de maintenance des services des TI.

ANNEXE 1 – Accès à la structure pour l'externe

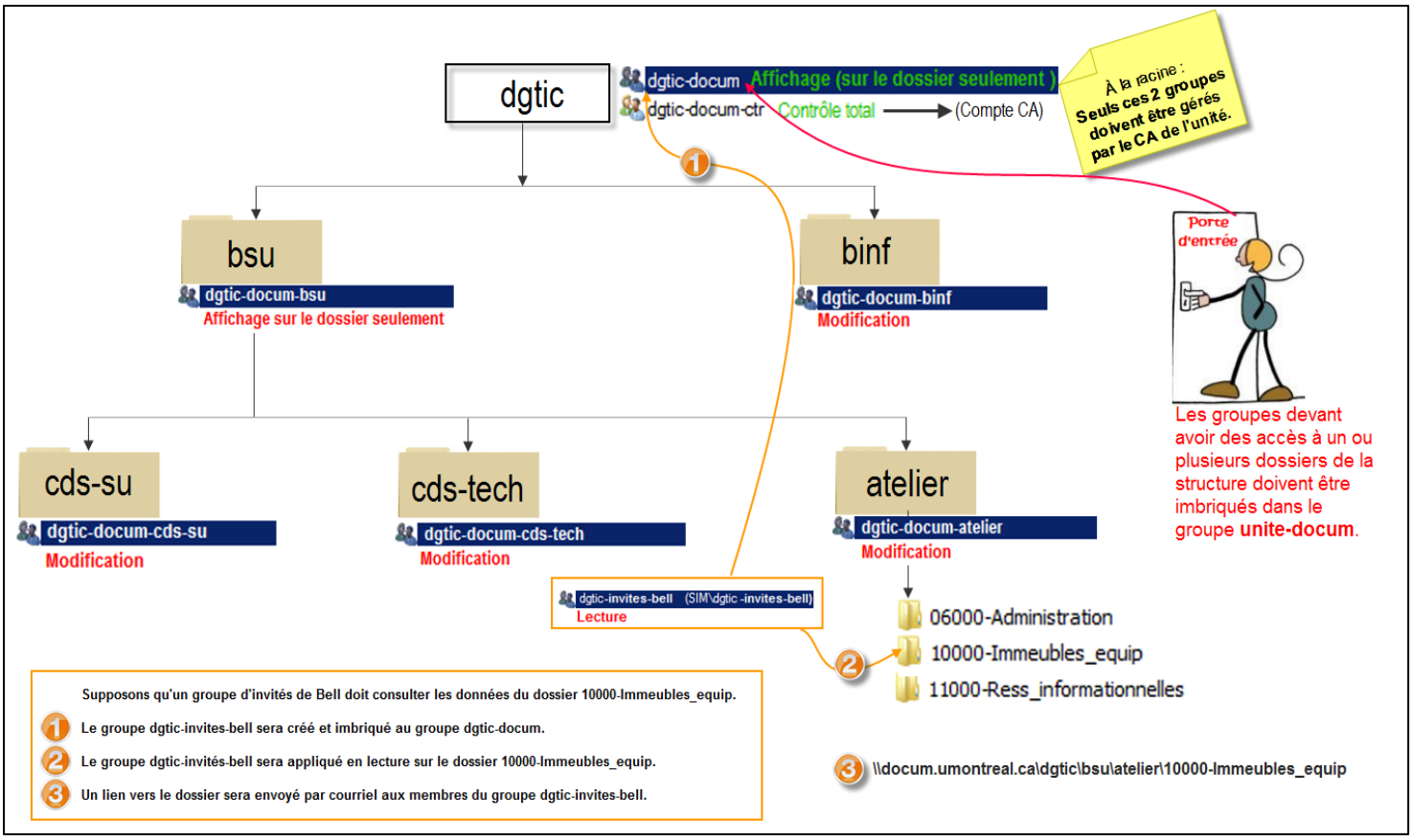
Dans des cas particuliers seulement, il arrive que des permissions doivent être données à des personnes de l'extérieur. Il peut s'agir d'invité(s) ou de membre(s) d'une autre unité. Il est possible d'ouvrir l'accès. Le cas de figure suivant en démontrera la procédure.

Supposons qu'un groupe d'invités de Bell doivent consulter les données du dossier 10000-Immeubles-equip. Le groupe *dgtic-invites-bell* sera d'abord crée par l'OGLP et les invités y seront intégrés.

1) Le groupe *dgtic-invites-bell* sera imbriqué au groupe *dgtic-docum* qui se trouve à la racine de la structure seulement.
2) Les droits de **lecture** (ou autres) seront ensuite appliqués sur le dossier 10000-Immeubles_equip pour le groupe d'invités.
3) Un lien (ex : \\docum.umontreal.ca\dgtic\bsu\atelier\10000-Immeubles_equip) devra être envoyé aux invités par courriel afin de leur permettre d'accéder directement au dossier.

   Ceux-ci ne pourront jamais naviguer à l'intérieur de la structure.

Il est extrêmement important de garder trace de cette ouverture car elle devra être enlevée dès que le travail de collaboration sera terminé.

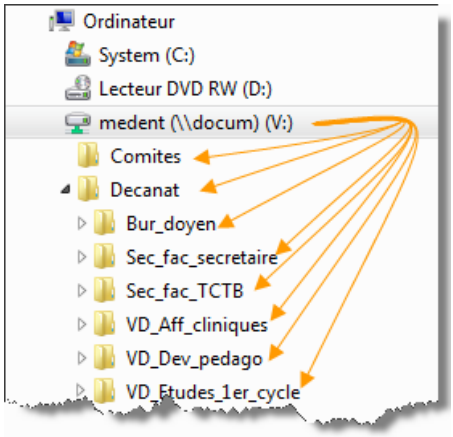


Cet exemple a été créé avec l'acronyme DGTIC avant que l'unité ne change de nom pour TI.

ANNEXE 2 – L'héritage

L'héritage – comment ça fonctionne ?

À moins d'autorisations spéciales, chaque dossier « Enfants » hérite des mêmes droits d'accès que son « Parent ».



Ainsi, dans l'exemple à gauche, l'espace « medent » étant le « Parent », tous ses « Enfants » (sous-dossiers) possèdent les mêmes droits d'accès puisque ceux-ci sont hérités du parent.

Pour le groupe ***unite-docum*** une autorisation spéciale est appliquée.

Il est extrêmement important de **NE JAMAIS COUPER L'HÉRITAGE**.

Risques importants lorsque l'héritage est coupé

Lorsque l'héritage est coupé, un groupe peut alors être supprimé.

1. Si les trois (3) groupes ci-après nommés étaient supprimés, comme leurs membres possèdent le contrôle total, ceux-ci perdraient automatiquement tous les droits de gestion sur tous les sous-dossiers à partir du dossier où l'héritage a été coupé.
   - ***Domain admin*** *(Réservé aux TI)*
   - ***docum-ctr*** *(Réservé aux ti)*
   - ***unite-docum-ctr*** (Réservé au coadministrateur de l'unité)

   La personne responsable d'appliquer les droits d'accès pourrait très facilement s'enlever les droits de gérer les permissions sur ses propres dossiers.

2. Si le groupe nommé ***unite-docum*** était supprimé, les membres de tous les groupes y étant imbriqués ne pourraient plus naviguer dans la structure.

Autres conséquences d'un héritage coupé

Pour toute sorte de raisons techniques, il arrive fréquemment qu'il faille ajouter de nouveaux groupes d'accès sur la structure. Ces nouvelles permissions peuvent être appliquées sur le dossier racine ou sur des dossiers spécifiques sous la racine.

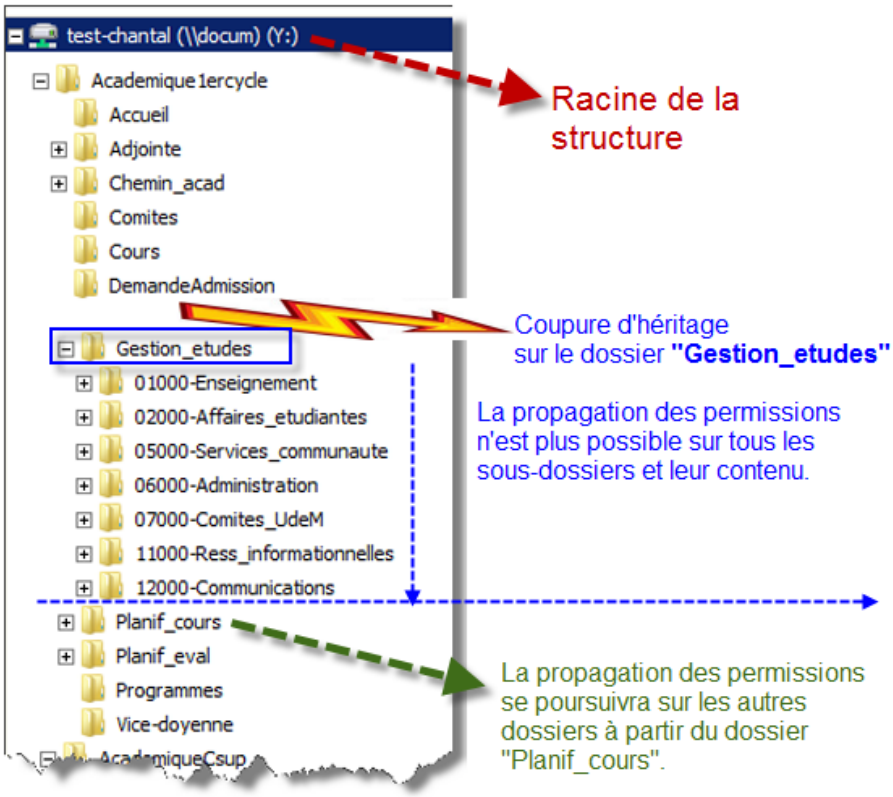
S'il y a plusieurs coupures d'héritage sur la structure, il devient très difficile, voire impossible, de se rappeler à quels endroits les coupures ont été faites.

Comment le responsable pourrait-il :

- Retracer quels sont les dossiers qui n'héritent plus des permissions des niveaux supérieurs ?
- Tenir à jour quelles sont les permissions spécifiques des dossiers de la structure en général ?
- Maintenir la simplicité souhaitée dans l'application des permissions ?
- Léguer les particularités de ces permissions à son successeur ?

Dans l'exemple à droite une coupure d'héritage est faite à partir du dossier « Gestion_etudes ».

Supposons qu'il faille ajouter un nouveau groupe devant obtenir des droits d'accès sur toute la structure, il serait alors impossible de savoir que le dossier « Gestion_etudes » et tous ses enfants n'hériteraient pas de ces nouvelles permissions.

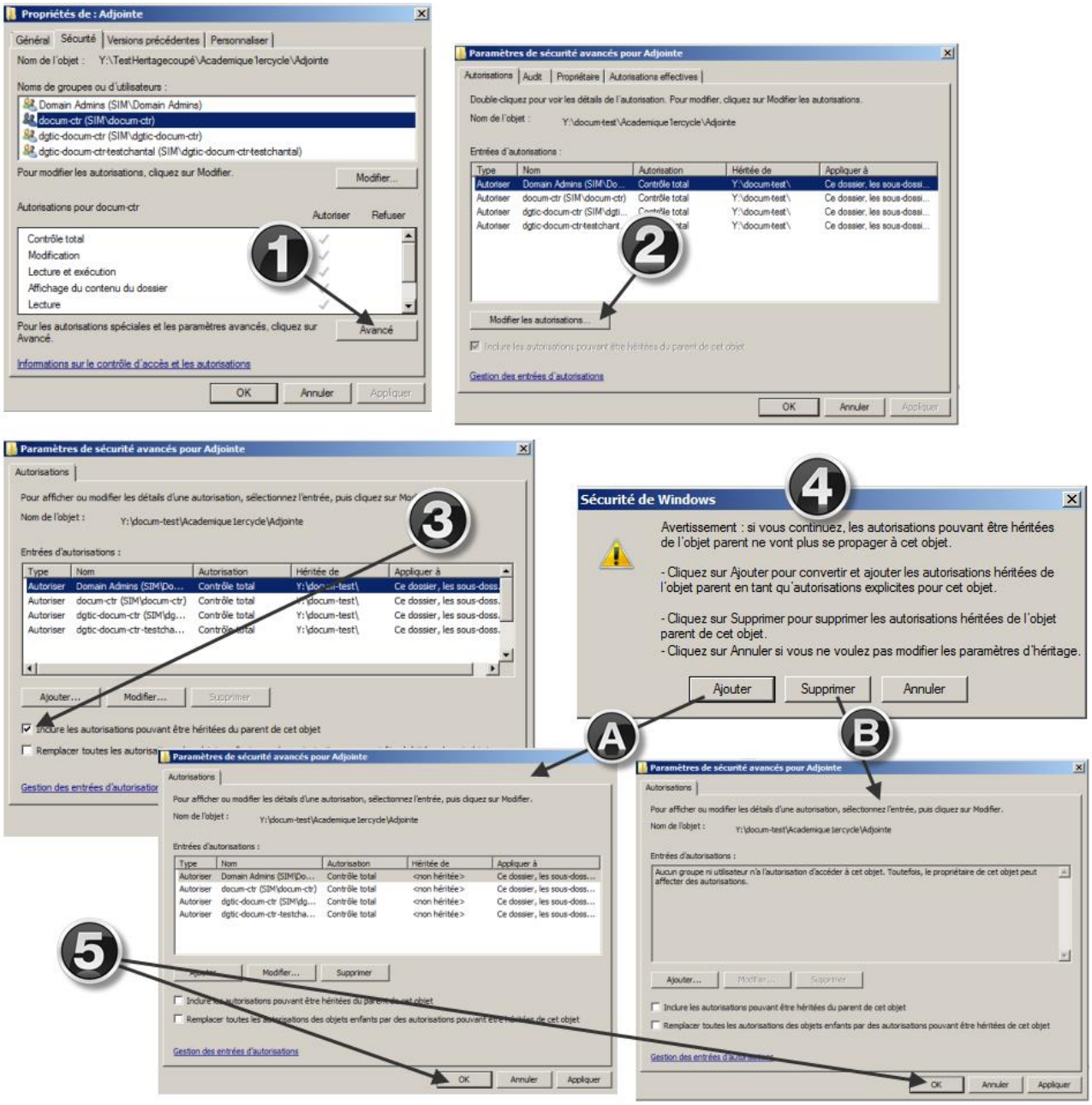


Procédure pour couper un héritage (non recommandé dans l'application du modèle proposé)

Nous expliquons la procédure ici seulement pour mieux sensibiliser les utilisateurs que les manœuvres non-désirées sont faciles à faire lorsque l'on coupe l'héritage.

Une fois dans les propriétés du dossier :

1) Cliquer sur *Avancé.*
2) *Modifier les autorisations*.
3) Décocher la case *Inclure les autorisations pouvant être héritées du parent de cet objet*.
4) A) Si l'utilisateur clique sur *Ajouter*, les groupes listés seront copiés et l'héritage sera coupé.
   B) Si l'utilisateur clique sur *Supprimer*, tous les groupes listés seront supprimés et l'héritage sera coupé. – **TRÈS DANGEREUX CAR PLUS PERSONNE N'AURA ACCÈS AUX DOSSIERS**.
5) OK

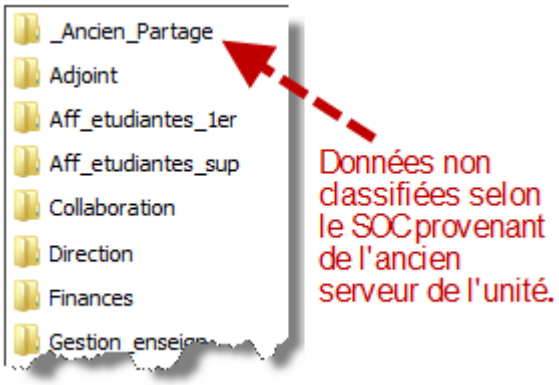


ANNEXE 3 – Message important concernant la migration

Il est possible de migrer les données d'une unité de différentes façons. Le type de migration sera déterminé par la responsable du projet qui pourra évaluer les besoins individuellement.

Un dossier nommé « _Ancien_Partage »

Si les données n'ont pas toutes été reclassées selon le système officiel de classification (SOC)[1] avant la date de migration, alors les données seront migrées en incluant un dossier nommé «_ Ancien_Partage ». Les employés de l'unité devront poursuivre la démarche de classification et ainsi vider ce dossier. Celui-ci devra, être détruit une fois vidé.



Mise à part l'accès en modification, les permissions d'accès appliquées sur le dossier «_Ancien_Partage » sont les mêmes qu'avant la migration de sorte que les utilisateurs ne pourront pas ajouter d'autres fichiers mais pourront seulement les transférer *(copier/coller/supprimer)* dans le dossier approprié plus bas dans la structure.

Les utilisateurs ne doivent pas **DÉPLACER** les éléments mais doivent plutôt les **COPIER** et les **COLLER** dans le bon dossier pour ensuite les **SUPPRIMER** du dossier « _Ancien_Partage ».

Sans cette manœuvre les anciennes permissions d'accès pourraient être copiées dans la nouvelle structure; CE QUI N'EST PAS SOUHAITABLE.

[1] Se référer au guide « Partage de fichiers dans DocUM » pour obtenir plus de détails.